

# Critical Infrastructure and Control Systems Security Curriculum

DRAFT Version 1.0

*February 28, 2007*

## **Authors**

Philip Auerswald  
*George Mason University*

Lewis Branscomb  
*University of California San Diego and Harvard University*

Michael Kleeman  
*University of California San Diego*

Todd M. La Porte  
*George Mason University*

Ryan N. Ellis  
*University of California San Diego*

## **Principal Investigators**

Susan Shirk  
*University of California San Diego*

Philip Auerswald  
*George Mason University*



# Homeland Security

## Control Systems Security Program



**CONTENTS**

Introduction..... 3

Content of the Course ..... 5

Module 1: Vulnerability of Critical Infrastructure (CI) ..... 6

    Session 1 – Awareness ..... 7

    Session 2 -- Concepts ..... 7

    Session 3 – Training ..... 8

    Session 4 – Actions ..... 8

Module 2 – Engineering Approaches..... 10

    Session 1 – Awareness ..... 10

    Session 2 – Concepts ..... 11

    Session 3 – Training ..... 11

    Session 4 – Actions ..... 12

Module 3: Managing Organizations and Risk ..... 13

    Session 1 – Awareness ..... 13

    Session 2 – Concepts ..... 14

    Session 3 – Training ..... 15

    Session 4 – Actions ..... 15

Module 4: Securing Networks of Enterprises ..... 17

    Session 1 – Awareness ..... 17

    Session 2 – Concepts ..... 18

    Session 3 – Training ..... 18

    Session 4 – Actions ..... 19

Module 5: Creating Markets ..... 20

    Session 1 – Awareness ..... 20

    Session 2 – Concepts ..... 21

# Critical Infrastructure and Control Systems Security Curriculum

Session 3 – Training .....	21
Session 4 – Actions .....	22
Module 6: Building Trust – Public/Private Policy .....	23
Session 1 – Awareness .....	24
Session 2 – Concepts .....	24
Session 3 – Training .....	25
Session 4 – Actions .....	25
Appendix A Modular Design .....	A-1
Appendix B Annotated Bibliography .....	B-1
Appendix C Key Government Reports .....	C-1

# Critical Infrastructure and Control Systems Security Curriculum

Tools to create a masters-level course on the security and resilience of critical infrastructures with emphasis on control systems security

This document is designed to assist those who wish to teach a course on the public policies, technical issues, and managerial principles required to achieve and sustain robustness and resilience of critical infrastructure services that may be threatened by disasters of many kinds. This material can be applied to a broad range of infrastructures, their technology systems, and kinds of threats to which they may be exposed, but this material draws primarily on the role of control systems in energy, cyber, and other infrastructures. It provides materials from which instructors can design a specific syllabus to meet the needs and requirements of their particular circumstances.

Course materials:

1. Devoted specifically to a range of critical infrastructure services and their interdependences.
2. Deal with “all hazards,” that is, not only terrorism, but natural disasters and the unintended consequences of accidents, poor management, results of inappropriate government regulatory policy, and inadequate technology and system designs.
3. Integrate the public policy tools for inducing private firms to invest in mitigation of threats and increasing resilience.
4. Discuss technical specifics about the vulnerabilities of critical infrastructure service delivery with special emphasis on those services dependent on control systems reliability and recoverability.
5. Recognize the international dimensions of both threats and solutions and examine alternative public/private relationships and modes of governance.
6. Explore the management and organizational experience of firms that have learned how to provide consistently high reliability in their service delivery.

This document may be copied and used for designing such courses. It is the user’s responsibility to respect all copyrighted material proposed as readings for the course. However, many of the readings have URLs that provide access to pdf files that we believe are offered for use without charge, unless stated otherwise. The books and government documents that are not available in electronic form are found in most research libraries. Most of the journal articles are found through JSTOR for which many universities are licensed. For further information, please contact Lewis Branscomb at <lbranscomb@ucsd.edu> and/or Philip Auerswald at <pauerswa@gmu.edu>.

The authors and leaders of this project are:

**Susan Shirk, PhD** is PI of the UCSD component of the project. Susan Shirk is Professor of Political Science at the Graduate School of International Relations and Pacific Studies (IR/PS) at UC San Diego. A former director of IGCC (1991–1997), Professor Shirk accepted an assignment at the U.S. Department of State in 1997 where she served as Deputy Assistant Secretary for China in the Bureau of East Asian and Pacific Affairs. Shirk returned from her three-year term at the U.S. State Department in 2000 to become an IGCC research director. <sshirk@ucsd.edu>

## Critical Infrastructure and Control Systems Security Curriculum

**Philip Auerswald, PhD** is PI of the George Mason University (GMU) component of the project and Director of the Center for Science and Technology Policy and an Assistant Professor at the School of Public Policy of GMU. Professor Auerswald's work focuses on linked processes of technological and organizational change in the contexts of policy, economics, and strategy. He is the co-editor of *Innovations: Technology | Governance | Globalization*, a quarterly journal from MIT Press about people using technology to address global challenges. <pauerswa@gmu.edu>

**Lewis M. Branscomb, PhD** is Professor of Public Policy and Corporate Management, emeritus, at Harvard University's Kennedy School of Government and now holds appointment as Adjunct Professor in International Relations and Pacific Studies at the University of California, San Diego. Dr. Branscomb was the co-chairman of the project team at the National Academies of Science and of Engineering and the Institute of Medicine, which authored the 2002 report *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. <lbranscomb@ucsd.edu>

**Michael Kleeman** is an independent consultant working in the technology and health related areas. During the last two years, he served as the Chief Technology Officer for Catenas, a network of professional services firms, and Aerie Networks, a new long-distance provider in the United States. Kleeman has over 25 years of experience in telecommunications and information systems related business strategy, technology design, economic analysis, and complex project management. He has also worked on the design and implementation of networks for voice and data communications, including carrier and private networks in both domestic and international arenas. He has extensive industry expertise in the technology/computer, commercial, government, financial, and health areas, both as a consultant and as an operating manager. <mkleeman@ucsd.edu>

**Todd M. La Porte, PhD** is an associate professor at George Mason University. He was a member of the Faculty of Technology, Policy, and Management at the Delft University of Technology in the Netherlands. Dr. La Porte also served for six years as an analyst in the information technology and the international security programs at the Office of Technology Assessment, a research office of the U.S. Congress. <tlaporte@gmu.edu>

**Ryan N. Ellis**, research fellow, is a doctoral student in the Department of Communication at the University of California, San Diego. He received his MA in Communication in 2004 also at the University of California, San Diego. His current research focuses on the history of competition within the U.S. postal industry and the contemporary politics of postal service. <rnellis@ucsd.edu>

The project is funded by the Department of Homeland Security Control System Security Program; contract administered by Idaho National Laboratory and Lawrence Livermore National Laboratory.

### **Acknowledgements:**

The project team is appreciative of the vision of Dr. Brian Lopez, Lawrence Livermore National Laboratory, who saw the value of such a project and provided valuable guidance throughout the work. We are also grateful to Dr. Raymond J. Clark, Program Manager for the "Public Policy and Biological Threats" program of the University of California Institute on Global Conflict and Cooperation (IGCC). Dr. Clark provided critical guidance and support to the UCSD component of the project.

## Critical Infrastructure and Control Systems Security Awareness Curriculum

### Introduction

This curriculum is designed as a tool to be employed by an instructor for use in creating a masters-level professional course on Critical Infrastructure (CI) and Control Systems Security (CSS). The objective of any course constructed with this tool will be the same: to convey fundamental organizational and economic principles required to (1) effectively manage high-impact risk to infrastructure services, and (2) design and implement public policies and business strategies that mitigate such risks. Even though many of the case examples are drawn from control systems, the principles will apply to other CI situations.

The curriculum is also designed to be flexible. Instructors will need to accommodate a variety of constraints with regard to the course length, the number of meetings, the mix of student professional areas and skills, and the objectives of the institution offering such a course.

The subject is inherently interdisciplinary, and thus, the course is also. The course focuses on policymaking and decision strategies, in both public and private institutions. The risks faced are both managerial and technical. In addition, the tradeoffs between risk and reward are challenging matters in economics. Thus, it is assumed that the offering institution is most likely to be concerned with public policy and security studies, but students are expected to be drawn from multiple disciplines, including engineering, management, and economics.

#### *Public and private enterprise policy*

The policy context, within which both public and private decisions are taken, will be explicated throughout the course. The course will seek to expose *what* needs to be done by government and by CI firms, but importantly, *why* the resulting decisions and investments are not being made at this time. In other words, the course does not focus primarily on “what to do” or even on “how to do it,” but rather on “why society should -- and how society can -- cause the necessary actions to be taken.” The course also evaluates policy within the “all-hazards” context, focusing on catastrophic events of both natural and man-made origin.

#### *A modular design for the course*

Appendix A is an Excel template that defines six areas to be covered in the sequence specified, each in some depth. These are referred to as modules. Each module will cover four activities called “sessions.” Sessions, discussed below, are *not* meant to define class meetings; the specific syllabus will be tailored by each instructor to schedule time for review, exams, possible field trips for casework, and other activities.

The division of session material into lectures will depend both on the number of lectures comprising a given course and the duration and frequency of lectures. However, the functions served by each of the four sessions in each module are expected to be covered. Goals for each are specified, as are readings and plans for class exercises or case discussions.

This modular architecture is designed to meet two challenges:

1. Institutions vary in the number of weeks in a course (10-week trimesters; 15-week semesters, typically). The Excel template in Appendix A defines the six basic modules of the course, with four sessions each. If each session did represent a class session, 24 such meetings would be required. To fit six modules into a 10-week quarter, each module would have to be covered in 1.7 weeks on

## Critical Infrastructure and Control Systems Security Curriculum

average. In a 15-week semester, the six modules can expand to 2.5 weeks/module, which could be achieved with two classes per week.

2. This is an interdisciplinary course; no two versions of this course will have the same ratio of disciplines, nor will they have the same goals.

### *Modules*

#### **Module 1. Vulnerability of Critical Infrastructures (CI)**

The role of CI in the economy; identification of risks in prior White House studies; problem of private sector incentives in the face of security externalities; government assumption that markets are sufficient; the all-hazards, all scales approach (firm, industry, cross-industry); difficulty of defining risks; and the policy problem of defining accountability between government and private sector.

#### **Module 2. Engineering Approaches**

The opportunities and limits of engineered solutions to the CI challenge with a primer on technologies employed, their historic context, and current key issues. Principal emphasis is on control systems, including comparison and contrast with other scenarios.

#### **Module 3. Managing Organizations and Risk**

An examination of the opportunities and limits of management and organizational practices as tools to address CI challenges within the enterprise. Contrasting strategies to achieve assured high operations reliability focused on flexibility and responding to the unexpected, versus defining quantitatively the risks and means to reduce them individually.

#### **Module 4. Securing Networks of Enterprises**

The challenges of infrastructure interdependencies in multi-firm industries, and the relationship to the dependencies and organizational politics within firms as discussed in Module 3. Includes examination of the problems of accountability, inefficiencies from vertical integration to reduce risk of interdependence and recognition of global interdependencies (in supply chains, for example).

#### **Module 5. Creating Markets**

Limits of market-based approaches to addressing CI challenges and policy opportunities for overcoming these limitations. Emphasis on policy tools available to government, such as incentives for insurance and re-insurance industries, defined legal vulnerabilities, cost shared investments in R&D, and validation.

#### **Module 6. Building Trust—Public/Private Policy**

Pathways toward reciprocity and collective action in addressing the CI challenge. Focus on economic trends toward infrastructure services as a growing fraction of a high-tech competitive economy; theories for defining government, shared public-private, and private roles; and sources of potential leadership to set the society on a long-term course of higher reliability and resilience of critical services.

# Critical Infrastructure and Control Systems Security Curriculum

## *Sessions*

Each module is to be addressed by four sequential activities (sessions).

**Session 1. *Awareness*** defines and scopes the issues in the module, stressing why this module is a necessary addition to those before and defining the issues to be addressed. (These first sessions in each module provide an overview of one sixth of the material, and might be assembled into a one-week short course.)

**Session 2. *Concepts*** is the pedagogical session introducing the basic, specialized knowledge about the module (whether it concerns engineering, economics, management, policy studies, etc.), designed to provide a class of students with diverse backgrounds a common basis in understanding.

**Session 3. *Training*** is the session where the class is expected to deal with a problem situation in a realistic context. This might be a case example, and in some instances, could involve a site visit to a firm to which the case is applicable. Different modules would use this time differently. In some cases (such as Module 5, Creating Markets), the exercise might be an economic analysis or some other form of practical exercise.

**Session 4. *Actions*** is the take-away session, with the class led to appreciate that the situation they just studied needs to be informed by the forthcoming modules. Thus, Session 4 consolidates the background to introduce the next module.

## **Content of the Course**

Each module contains:

- a. A short essay describing the motivation and objectives of that module and how it draws on the prior modules, including at least three basic questions that the module seeks to explicate.
- b. An introduction to the pedagogical material required for that module.
- c. A plan for the case or exercise to be used in Session 3 of the module.
- d. The groundwork for the next module.

A small number of required readings (typically not more than three) will be provided for each session of the module.

In addition, Appendix B contains an expanded annotated bibliography that includes all of the required readings and references to recommended further reading for each module. Appendix C contains URLs to the major government documents likely to be referenced in this course.

## **Module I: Vulnerability of Critical Infrastructure (CI)**

Critical infrastructure (CI) services are and will continue to be increasingly important in the economy, despite their vulnerability to high consequence events arising from threats of terrorism, national disasters, and service failures such as the Northeast power blackout in 2003. As all firms drive for economic efficiency by outsourcing services, the robustness and resilience of critical infrastructures is increasingly at risk.

Understanding how the loss of resilience that typically follows from strenuous response to competitive pressures is a central task of this module. It is central to the Hobson's choice of losing competitive position at the expense of risking disaster. In the reading from Lovins and Lovins, we are reminded that some insightful authors devoted to what today might be called "green technology" anticipated a quarter-century ago both the vulnerability and the lack of resilience in over-centralized, excessive-scale technologies.

The second task of this module is to understand the history of government concern with the viability of critical infrastructures (and their underlying control systems), starting in the early 1990s. The White House commissioned a number of studies of such potential disasters and asked how the risks of disaster might be mitigated by public policies. Recognizing that most CI industries are in the private sector, the U.S. government has assumed that markets will provide sufficient incentives to induce the needed private investments to defend against such risks. (See the National Infrastructure Protection Plan, NIPP.) This result has not been achieved, since the risks of catastrophes are, in most cases, extremely difficult to quantify, especially in the case of terrorism.

Thus, the task of reducing vulnerability of critical infrastructure firms remains a difficult-to-solve problem. The terrorist attack of September 11, 2001 greatly raised the visibility of these issues, resulting in the amalgamation of a large number of federal agencies into the Department of Homeland Security.

The third task of this module is to introduce a number of the basic ideas that underlie the strategies for assuring availability of services in time of disaster. These ideas include the concepts of resilience, robustness, risk, and vulnerability. Pat Longstaff offers a discussion of resilience and robustness, while Brian Lopez provides an in-depth introduction to risk and vulnerability as it relates to CI. We discuss economic concepts that underlie the effect of rising efficiency on falling resilience, understand security externalities, and their affect on investment decisions and address the circumstances under which insurance can induce vulnerability reducing investments.

Module 1 will explore the merits of an "all-hazards" approach (service failures, natural disasters, and terrorism) understood at all scales (one firm, an industry, cross-industry, and inter-infrastructure industries). The sources of vulnerability of CI industries, which are largely technical *and* managerial, have been studied at some length but still are not well understood. Indeed, it is difficult to rigidly separate technical and managerial questions; the next module provides a primer on some of these issues in relation to Critical Infrastructure Protection (CIP).

But, the difficulty of defining risk for rare events of high consequence exacerbates the policy problem of defining accountability between government and private sector. Thus, an unusual degree of agreement and cooperation between government and the industries that it regulates in varying degrees becomes a major challenge. For this reason, the study of collaborative governance is an important baseline for thinking about the public policy choices that are revisited in Module 6.

# Critical Infrastructure and Control Systems Security Curriculum

## ***Session 1 – Awareness***

### Objectives:

Understand the historical context of the tolerance of very rare but catastrophic events on the part of service industries and the unrealistic assumption by government that markets will adequately motivate the required private investments to reduce vulnerability significantly.

### Key questions:

1. How has the role of federal government changed with relation to CI industries' vulnerability to terrorism?
2. What are the benefits and drawbacks of an all-hazards approach to federal disaster policy?

### Readings:

- \* United States. Department of Homeland Security. "Executive Summary." *National Infrastructure Protection Plan*. Washington, DC: 2006. 15-20.
- \* Flynn, Stephen E. "The Neglected Home Front." *Foreign Affairs* 83.1 (2004): 20–33.
- \* Homer-Dixon, Thomas. "The Rise of Complex Terrorism." *Foreign Policy* 128 (Jan./Feb. 2002): 52-62.
- \* Branscomb, Lewis M. "A Nation Forewarned: Vulnerability of Critical Infrastructure in the 21<sup>st</sup> Century." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerwald et al. New York: Cambridge UP, 2006. 19-25.
- \* Lovins, Amory B. and L. Hunter Lovins. "National Energy Insecurity." *Brittle Power: Energy Strategy for National Security*. Andover MA: Brick House Publishing Cop., 1982. 1- 10.

## ***Session 2 -- Concepts***

### Objectives:

- Explore the economic concepts that underlie the effect of rising efficiency on falling resilience.
- Understand security externalities and their effect on investment decisions, and address the circumstances under which insurance can induce vulnerability-reducing investments. Understand the concepts of resiliency, robustness, and reliability.
- Explore the political-economic environment within which infrastructure service firms must compete and cooperate with other firms sharing the same service role.
- Understand the balance of self- and imposed regulation of these industries, and the effect of this balance on prospects for public-private cooperation in reducing catastrophic risks.
- Explore the possibilities for public policies based on collaborative governance.

### Key questions:

1. Under what circumstances do firms in a service industry both compete and cooperate effectively? Is resilience always a casualty of increasing efficiency?
2. What factors govern a firm's willingness to invest in vulnerability reduction when facing very low risks of serious consequence?
3. What is the political-economic context for seeking government-industry collaboration in creating and executing an effective CI protection policy?

## Critical Infrastructure and Control Systems Security Curriculum

### Readings:

- \* Donahue, John D. “On Collaborative Governance.” CSRI Working Paper Series #2 (Feb. 2004). Cambridge, MA: Kennedy School of Government, Harvard University.
- \* Longstaff, Pat. *Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology*. Program on Information Resource Policy, Harvard University, 2005. 1-42.
- \* Lopez, Brian. “Evolution of Vulnerability Assessment Methods.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerwald et al. New York: Cambridge UP, 2006. 51-68.
- \* Auerwald, Philip, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, “Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerwald et al. New York: Cambridge UP, 2006. 3-12.

### **Session 3 – Training**

#### Exercise:

Create mixed discipline teams of students. Ask them to consider the example of the electrical energy industry, a critical infrastructure service whose reliability and resilience are threatened by expanding government deregulation, and where management goals diverge from promoting security and the reduction of vulnerability in an environment where risk cannot be quantified. Discuss how corporate executives who feel strong competitive pressure would make decisions about such investments, including how they might go about estimating risks, costs and benefits and how they might be influenced by decisions of their competitors (who may face same vulnerability but different risks).

#### Readings:

- \* Committee on Science and Technology in Countering Terrorism, National Research Council. “Energy Systems.” *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academies Press, 2002. 177 – 209.
- \* Nevius, David R. and Ellen P. Vanco. “Ensuring a Reliable North American Electric System in a Competitive Market Place.” Prepared for the U. S. – Canada Power System Outage Task Force. 15 Aug. 2005.

### **Session 4 – Actions**

#### Objectives:

Prospective view of the issues that must be confronted in Module 2: technical sources of vulnerability; assessing vulnerabilities and risks; managing high-reliability; conditions for creating and maintaining resilient enterprises. Understanding the important role of information technology in general and control systems in particular. Emphasizing the importance of addressing both management and technology issues simultaneously.

#### Key questions:

1. How well structured is the U.S. government for addressing those issues (such as CI protection) where information technology (including very complex and specialized control system technology) is especially important?

## Critical Infrastructure and Control Systems Security Curriculum

2. What resources are available in industry and in government, and how do they compare and relate?
3. What do the appropriate policies for two classes of disaster have in common: (a) disasters caused by either terrorists or nature, and (b) disasters caused by some combination of poor management, wrong engineering, and regulatory environments inappropriate to high resilience?

### Readings:

- \* Committee on Science and Technology in Countering Terrorism, National Research Council. "Executive Summary." *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press, 2002. 1-24.
- \* Committee on Science and Technology in Countering Terrorism, National Research Council. "Information Technologies," *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press, 2002. 135-176.

## Module 2 – Engineering Approaches

Critical Infrastructures evolve over time, with changes in architectures and components driven by technology and operational changes. These changes drive down costs and increase the utility of all infrastructures, but the most dramatic change has been in computer-based environments, which have impacted all aspects of the economy from office work to aircraft control. Computer-based Supervisory Control and Data Acquisition (SCADA) systems and process control systems are utilized in almost all critical infrastructure sectors, and essential to their reliable performance. These systems monitor and control processes and provide a human interface to permit operator interaction.

In the past, SCADA systems were typically highly customized with hardware, software, and network protocols designed specifically for each system. In the last 15 years, systems have been built using standard commercial off-the-shelf (COTS) components and software built on standard operating systems and network protocols. The growth of standards-based environments, especially the adoption of off-the-shelf systems and internet protocols, has led to the spread of these systems across industries, while at the same time increased their vulnerabilities to failure from accidents or attack.

Decisions regarding any critical infrastructure environments are complex, with a series of functional (including security) and economic tradeoffs. Nowhere are these decisions more complex than in computer-based environments such as SCADA, where the risks are hard to determine and the benefits of increased functionality, security, or optimization are hard for management to determine.

This module will examine these complex issues starting with primers on critical infrastructure and control environment technologies, and moving to an evaluation of what can go wrong when management underestimates the risks of lack of full functionality in a SCADA environment, in this case, risking a nuclear reactor meltdown. The readings will start with a look at SCADA in critical infrastructure from the view of the Government Accountability Office (GAO). They will move to a more technical look at electrical grid monitoring and control, and will conclude with a primer (Shaw) on SCADA and computer security.

Some of the technological issues raised by increased use of standardized components (esoteric systems are harder to attack) will be considered. The systemic impact of these systems in the critical telecommunications infrastructure is explored in a recent report from Congress. Part of the goal of this module is to raise the issue of the relationship of technology and management decision-making, which is examined further in the next module.

For further readings on control systems operation and risk, as well as sector-specific discussions of the use of control systems, see the supplementary readings provided in Appendix B, Module 2.

### *Session 1 – Awareness*

Objectives:

Understand the key technologies underlying critical control infrastructures in various industries in the United States and the design considerations for these systems in light of threats of natural or man-made catastrophic events.

Key questions:

1. What are the key technologies that underlie critical infrastructure control in the United States?
2. What are SCADA systems and why were they developed?

## Critical Infrastructure and Control Systems Security Curriculum

3. What are the key vulnerabilities of these technologies in light of the range of threats from all hazards?

### Readings:

- \* Apt, J., L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic. "Electrical Blackouts: A Systemic Problem." *Issues in Science and Technology* 20.4 (2004): 55–61.
- \* United States. General Accounting Office. "Critical Infrastructure Protection: Challenge and Efforts to Secure Control Systems." GAO-04-354. Mar. 2004. Washington, DC.
- \* Shaw, William. *Cybersecurity for SCADA Systems*. Tulsa, OK: PennWell, 2006.

### ***Session 2 – Concepts***

#### Objectives:

- Explore the underlying technological and economic drivers of SCADA control systems and how they have evolved as a result of changes in computer and network technology.
- Understand how these changes, along with formal and informal standards, have affected, both positively and negatively, the vulnerability of these systems.

#### Key questions:

1. How have computerized systems expanded their role in various critical infrastructure providers?
2. What are the changes in the off-the-shelf technology, hardware, software, and network and how have these changed the capabilities and vulnerabilities of SCADA systems?
3. How have the risks of intrusion or failure increased as a result of network connectivity and standards?

#### Readings:

- \* Nash, Troy. "Backdoors and Holes in Network Perimeters." US-CERT Control Systems Security Center. Case Study Series Vol. 1.1 (2005).
- \* Nash, Troy. "An Undirected Attack Against Critical Infrastructure." US-CERT Control Systems Security Center. Case Study Series Vol. 1.2 (2005).
- \* United States. Cong. House. Committee on Governmental Reform. *Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure*. Hearing, 30 Mar. 2004. 108<sup>th</sup> Cong. 2<sup>nd</sup> sess.
- \* Permann, May Robin, and Kenneth Rohde. "Cyber Assessment Methods." *InTech* 1 Nov. 2005.

### ***Session 3 – Training***

#### Objectives:

Operator training in control systems is as important as the system technology. The level of education and training of operators is a crucial variable in how the critical infrastructures that are controlled by such systems respond to failure, both local and general as in the case of high altitude electro-magnetic pulse (HEMP). This exercise is meant to help the students explore the differences in managerial philosophy between the owner of the Three Mile Island (TMI) nuclear power plant and the U.S. Navy in training on nuclear reactors, and generate a dialog about wide-scale systemic risks generated by a HEMP attack.

## Critical Infrastructure and Control Systems Security Curriculum

### Exercise:

Separate the class into two groups where half of the class portrays the operators at TMI and the other half portrays the nuclear engineers from the U.S. Navy. Ask each group to explain their training, mission, and career objectives. The instructor will then walk through two scenarios with the students where both groups are asked about their readiness training and then what tools and training they had received for a system failure. Then ask for a discussion on what the impact of a HEMP would be on each of their power systems and why they would potentially differ.

### Readings:

- \* Nuclear Regulatory Commission. *Three Mile Island: A Report to the Commissioners and to the Public*. Washington, DC: 1980. 1-26.
- \* U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the US and Canada*. Apr. 2004. 1-22.
- \* Sweet, William. "The Blackout of 2003." *IEEE Spectrum*. Aug. 2003.
- \* Foster, John S., et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report*. Washington, DC: Report to Congress, 2004.
- \* United States. Cong. Testimony of Vice Admiral Hyman George Rickover, *Naval Nuclear Propulsion Program--1972-73*, U.S. Hearing, 8 Feb. 1972 and 28 Mar. 1973. 92<sup>nd</sup> Cong., 1<sup>st</sup> sess. Washington, DC: Govt. Print. Office, 1974. 1-35.

### ***Session 4 – Actions***

#### Objectives:

The technologies of SCADA and other control systems are procured and operated in an environment of economic and managerial choice. Here the students will be able to examine the tradeoffs made by managers and the kinds of tools they have to make decisions about investment and operations.

#### Key questions:

1. How can non-technical managers evaluate technical risk, comparing the variety of hazards such as natural disasters, terrorism and human error?
2. What is right, and wrong, with the current models of economic analysis?
3. How can the increased cost of CIP be justified and managed?

#### Readings:

- \* Nuclear Regulatory Commission. *Three Mile Island: A Report to the Commissioners and to the Public*. Washington, DC: 1980. 89-108, 161-164.
- \* Schneier, Bruce. "Non-Security Considerations in Security Decisions." *Workshop on Economics and Information Security*, 29-30 May 2003.

## **Module 3: Managing Organizations and Risk**

This module focuses on the management challenges likely to be encountered in protecting critical infrastructures against disruption, whether from natural, technological, or terrorist sources. "Keeping the lights on," no matter what, is a colossal task, mostly performed out of public sight, except when problems arise, as with the blackout of 2003, and of course Hurricanes Katrina and Rita in 2005. As was covered in Module 2, this task has been impacted by technological changes in the past 20 years and strongly influenced by management decisions on technology.

System designers and operators struggle to balance the requirements of highly reliable, real-time operations against the demand of increasingly efficient and cost-effective service, where operating margins are cut to the bone in a deregulated environment. Terrorism only adds to the challenge, because attackers seek vulnerabilities, communicate with one another, and learn to defeat defensive measures.

The sessions in this module are designed to raise awareness of the nature of large technical systems and their distinctive operational characteristics, as described by specialists in organization theory and design. In particular, students will work with the key concepts that describe these organizations, looking at their internal structure and dynamics, but also crucially their political and institutional contexts. These conceptual lessons will be put to the test in the training exercise, which will be a simulation involving designers of a hypothetical critical infrastructure, its day-to-day operators, and an attacker group who will observe the design and operation and then try to disrupt the system.

By the conclusion of the module, students will have a clear understanding of the tradeoffs between security, reliability and efficiency, and the extraordinary challenges of managing complex critical systems in a turbulent and sometimes hostile world. They should also be prepared to discuss the added complexity of investment and management in systems and procedures that span multiple organizations, a topic of the next module.

### ***Session 1 – Awareness***

Objectives:

To consider the characteristics of critical infrastructures and the challenges they face. To understand the special properties and dynamics of large technical systems, and the debates about "normal accidents" (Perrow) and highly reliable organizations (HROs) with their extremely demanding requirements for management and operations.

Key questions:

1. What are the technical, organizational, and social implications of attempting to reduce failure to zero? What is the economic cost of doing so?
2. In complex technological and organizational settings, where powerful, risky, or essential systems are being operated in dynamic and/or turbulent environments, how can risk assessment techniques best be used? Do they have limitations? If so, how should such limitations be addressed by organization managers?
3. If failure is unacceptable in managing such complex and critical systems, and if trial and error learning is therefore not useful, what tools, perspectives, and/or methods can managers use to minimize risks to their systems and to the society that relies on them? How applicable are traditional management techniques in such situations? How would your answer have to change to take suicide terrorist actions into account?

## Critical Infrastructure and Control Systems Security Curriculum

### Readings:

- \* La Porte, Todd R. "Challenges of Assuring High Reliability When Facing Suicide Terrorism." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 99-120.
- \* Weick, Karl E., Kathleen M. Sutcliffe, Robert E. Quinn. *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. New York: John Wiley & Sons, 2001. 1-84.

### **Session 2 – Concepts**

#### Objectives:

Session 2 focuses on fundamental concepts in the study of organizations, particularly those that perform with extraordinarily reliability.

- Students will discuss the fundamentals of organization strategy, structure and behavior (La Porte), emphasizing the contrast between tightly-coupled, hierarchical, and linear-type systems with those that use more loosely-coupled, nonhierarchical, nonlinear, and interactive structures and procedures (Perrow).
- They will consider the strategic uses of *anticipation* and of *resilience* (Wildavsky).
- Finally, the session will introduce the topic of system design in the context of the need for highly reliable operations in contingent circumstances.

#### Key questions:

1. While the characteristics of highly reliable organizations can be sketched easily, their adoption in organizations is much more challenging. After outlining the main characteristics of highly reliable or "mindful" organizations, assess to what extent they exist in specific critical infrastructure or homeland security organizations. What are the challenges to managers of adopting structures or practices that would result in improved reliability or mindfulness?
2. Most critical technical systems (such as the SCADA systems discussed in Module 2) are designed and operated by different people who are working with different assumptions and different objectives. Some systems are so complex that seemingly no single person really understands them. How do risk, vulnerability, consequence, and design flaws get identified and addressed in such situations? What impediments are there to making improvements?
3. Most highly reliable or mindful organizations operate with generous resources, a strong collegial organizational culture, and substantial external support, whether in public or private sectors. What are the external political requirements for operating highly reliable, mindful, or essential systems? How can these conditions be sustained over long periods? What might happen if these conditions change?

#### Readings:

- \* La Porte, Todd M. "Organizational Strategies for Complex Systems Resilience, Reliability, and Adaptation." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 35-153.
- \* Perrow, Charles. "Complexity, Coupling and Catastrophe" and "Living with High Risk Systems." *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, 1984/1999. 62-100; 304-352.

## Critical Infrastructure and Control Systems Security Curriculum

- \* Wildavsky, Aaron. “Anticipation and Resilience” and “The Secret of Safety Lies in Danger.” *Searching for Safety*. New Brunswick, NJ: Transaction Books, 1988. 77-95; 205-228.

### ***Session 3 – Training***

Exercise:

The system design problem introduced in Session 2 will be further interrogated through a tabletop simulation. The exercise will result in increased awareness in each group of the perspective, interests, and concerns of the other groups, to encourage better designs, both for normal operations and during extreme events such as widespread blackouts or a terrorist attack. Teams will play the roles of “systems designers,” “operators,” and “attackers” in an iterative table-top simulation of the dynamics of systems design, systems operation, and terrorist or other attack with special emphasis on system reliability during extreme events or stress.

Readings:

- \* Schulman, P.R., E. Roe, M. van Eeten, and M. de Bruijne. “High Reliability and the Management of Critical Infrastructures.” *Journal of Contingencies and Crisis Management* 12.11. (2004): 14-28.
- \* Roe, E., et. al. 2002. *California’s Energy Restructuring: The Challenge to Providing Service and Grid Reliability*. EPRI, Palo Alto, California Energy Commission, Sacramento, CA. rpt. no. 1007388 (Dec. 2002).
- \* U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the US and Canada*. Apr. 2004. 1-173.

### ***Session 4 – Actions***

Objectives:

To help students develop a prospective view of management issues of highly reliable, complex, interdependent technical systems in turbulent environments, which are posited to be the future of all critical infrastructures. In light of the previous sessions, the group will discuss the tradeoffs and challenges of reconciling security, reliability, and efficiency of critical infrastructure systems in democratic societies. Readings by Perrow and Rochlin and the Columbia accident commission will provide some foundations for this discussion.

Key questions:

1. How can policy to reduce critical infrastructure vulnerability at the national level be designed to take into account the impacts of management practice and organizational structure on reliability?
2. How can the concept of resilience, either at the organizational, community, or national levels, most effectively inform policy for homeland security?
3. How do economic incentives for efficiency conflict with the need for reliability and security?

Readings:

- \* Perrow, Charles. “Organizing to Reduce the Vulnerabilities of Complexity.” *Journal of Contingencies and Crisis Management* 7.3 (1999): 150-156.
- \* United States. National Aeronautics and Space Administration. *Final Report of the Columbia Accident Investigation Board*. vol. 1. Washington, DC: 2003: chapters 5-8, 11.

## Critical Infrastructure and Control Systems Security Curriculum

\* Rochlin, Gene. 1997. *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton, NJ: Princeton University Press. See especially chapters 10-12.

## Module 4: Securing Networks of Enterprises

Networks, especially control networks, used to be limited to a single facility or organization. However, in the past 10 years we have seen the emergence of transnational and trans-organizational networks and control systems. These are seen in industries as diverse as electric power, oil and gas transport, and air transport and logistics. UPS now coordinates shipping and delivery operations directly with its customers, linking systems and creating a web of functionality and interdependence. Similar links occur in the energy systems, telecommunications networks, and air transport.

Understanding the evolution of these trans-organizational networks and the vulnerabilities they create will help the student understand how better to evaluate investments and the managerial requirements for their success. This will require an examination of the history of operational and then technical supply chain systems, how and why they can fail, and what business drivers impact decisions. Module 3 covered the management issues largely within organizations. Here these lessons will be applied in a multi-organizational context.

The background in this involved area will be integrated and examined in the context of failures and successes of complex distributed business systems. Nishiguchi's article examines what can go wrong with tightly linked systems and how they can recover. Lawler's piece from *Science* illustrates how NASA's optimized approach to development failed to meet expectations. The final session readings will then examine the specifics of tightly integrated networks (Greenstein on Internet economics, Gordon et al. on the question of economic versus functional optimization in cyber security, and Garcia and Horowitz in their piece on the policy and risks of under-investment). Module 5 will consider the effectiveness of market-based mechanisms.

### *Session 1 – Awareness*

Objectives:

To support the exploration of the interdependency of CI across players in a supply or value chain. See how a failure at one player ripples down the system and how the architecture of current hyper-optimized systems can lead to failures. Any system is only as secure as the least secure connected system with privileges.

Key questions:

1. What has led us to create these complex, geographically distributed, and vulnerable systems?
2. How have these created a more flexible and global business environment?
3. What are the risks associated with this business architecture?

Readings:

- \* Amin, M. "National Infrastructures as Complex Interactive Networks." *Automation, Control, and Complexity: An Integrated Approach*. Eds. Tariq Samad and John Weyrauch. New York: John Wiley & Sons, 2000. 263-286.
- \* Kinsey, Jean. "A Faster, Leaner, Supply Chain: New Uses of Information Technology." *American Journal of Agricultural Economics* 82.5 (Dec. 2000): 1123-1129.
- \* U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the US and Canada*. Apr. 2004. 131-153.
- \* Sheffi, Yossi. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press, 2005. 115-136; 270-285.

## Critical Infrastructure and Control Systems Security Curriculum

### ***Session 2 – Concepts***

Objectives:

- To understand the concepts of intra-organizational and inter-organizational networks and how they are part of today's complex supply and value chains.
- How these have been driven by the move towards economic optimization and how this impacts vulnerability.
- Explore system economics given certain assumptions (e.g., fuel costs).

Key questions:

1. Explain the concepts of optimization and hyper criticality.
2. What are the risks in the current extended supply chain systems?
3. How might a failure in one component propagate and how might it be minimized?

Readings:

- \* Carlson, J.M., and John Doyle. "Complexity and Robustness." *Proceedings of the National Academy of Sciences of the United States of America* 99.3 Suppl. 1 (2002): 2538-2545.
- \* United States. Department of Energy. *21 Steps to Improve Cyber Security of SCADA Networks*. Washington, DC: 2002.
- \* United States. Cong. House. Committee on Governmental Reform. *Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure*. Hearing, 30 Mar. 2004. 108<sup>th</sup> Cong., 2<sup>nd</sup> sess.
- \* St. Sauver, Joe. "SCADA Security and Critical Infrastructure." Eugene, OR: Infragaurd Meeting, 7 Dec. 2004.

### ***Session 3 – Training***

Objectives:

Control systems are complex environments with a number of interdependencies. The loss of a control system or operating environment can impact not only the party directly involved, but many others, and in the case of a major electrical outage, an entire geography. In order to give the students some idea of the cascading impacts of outage we will utilize a standard project management software tool such as SureTrak Project Manager in their PERT mode to illustrate critical path and inter-organizational impacts of disruption. We will also read about disruption and recovery in systems impacted by major disasters.

Exercise:

The instructor will divide the group into teams of three or four. The instructor will provide a basic template of the PERT chart with three corporate parties in a supply chain and within each of four system paths. One of these paths will cause major failures in supply and the others have redundancy. The students will complete these charts and operate the models under failure scenarios, describing the resulting impacts of up stream failures and recommending approaches to robustness. Also, the instructor will guide the students in a discussion on economic tradeoffs in robustness.

## Critical Infrastructure and Control Systems Security Curriculum

### Readings:

- \* Nishiguchi, Toshihiro, and Alexandre Beaudet. "Self-Organization and Clustered Control in the Toyota Group: Lessons from the Akin Fire." International Motor Vehicle Program, Massachusetts Institute of Technology, 1997.
- \* Lawler, Andrew. "Faster, Cheaper, Better on Trial." *Science* 288.5463 (2000): 32-34.
- \* Chatfield, Carl, and Timothy Johnson. Microsoft Office Project 2003: Step by Step. Redmond, WA: Microsoft Press, 2004.

### **Session 4 – Actions**

#### Objectives:

To examine the nature of the economics of the critical infrastructure protection issues. Who benefits from the current system and who bears the risks of failure. How do managers consider risk (discount), driven by their psychology, firm, and personal economic and other incentives.

#### Key questions:

1. Why might investments in critical infrastructure protection often be a lower priority than current profits?
2. To what extent can critical infrastructure and control systems security investments be justified on the basis of interdependency risks?
3. What are the incentives that might be changed to alter managerial behavior?
4. What is the market role and the role of regulation?

#### Readings:

- \* Greenstein, Shane M. "The Economic Geography of Internet Infrastructure in the United States." Working Paper #0046. Center for the Study of Industrial Organization, Northwestern University.
- \* Peterson, Dale, Matt Franz, and Landon Lewis. *SCADA Security*. Available Online: <[http://www.digitalbond.com/SCADA\\_Blog/SCADA\\_blog.htm](http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm)>.
- \* Gordon, Lawrence A., Martin A. Loeb, and William Lucyshyn. "Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets." 2<sup>nd</sup> Annual Workshop on Economics and Information Security, University of Maryland (2003).
- \* Garcia, Alfredo, and Barry Horowitz. "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy." The Fifth Workshop on the Economics of Information Security, Cambridge, UK (2006).

## Module 5: Creating Markets

Sound engineering and effective management can go a long way toward reducing operational vulnerabilities for a given company or government agency. However, as Module 4 of the course described, the fact that security investments and practices at one firm affect the vulnerability of other firms means that no institutional entity can address the infrastructure challenge on its own. Large numbers of firms that are geographically dispersed and in different industries require coordination.

In most of the world's economies, and certainly in the United States, markets are the default mechanism for achieving coordination. Decentralized markets successfully provide food, clothing, shelter, and essential services to most of the world's population. Markets manage risk and allocate investment. In recent years, markets have been created to address threats to health and societal wellbeing from local air pollution, resource depletion, and climate change. Other markets have been deregulated with the objective of achieving greater operational efficiencies and gain to consumers. It is natural, therefore, to consider how markets may be useful in addressing the critical infrastructure challenge.

Module 5 of the course is about the potential role of markets in addressing the critical infrastructure challenge. Students will gain an understanding of how markets can very effectively bring together and summarize information from many sources, distribute risk, and encourage investment. At the same time, students will acquire a better appreciation for the limits of markets. For example, markets function poorly when they involve few people, or when participants have a hard time agreeing on a price. These conditions apply to insurance and other markets that might otherwise be effective in coordinating private efforts to address the critical infrastructure challenge, and the role of policy, covered more completely in Module 6, has in impacting decisions.

### *Session 1 – Awareness*

Objectives:

To consider the potential effectiveness of markets in predicting future outcomes and addressing policy challenges characterized by poor quality public information. The session focuses on the creation of “information markets” to predict the outcomes of presidential elections and to assess the risk of terrorist attacks over time. Of particular interest are the prerequisites for the successful functioning of information markets, and strategies for their design.

Key questions:

1. How does terrorism challenge the role of markets in aggregating information?
2. What institutions are necessary for market functioning?

Readings:

- \* Hahn, Robert W., and Paul C. Tetlock. “Introduction to Information Markets.” *Information Markets: A New Way of Making Decisions*. Eds. Robert W. Hahn and Paul C. Tetlock. Washington, DC: AEI-Brookings Joint Center for Regulatory Studies, 2006. 1-12.
- \* Berg, Joyce E., and Thomas A. Rietz. “The Iowa Electronic Markets: Stylized Facts and Open Issues.” *Information Markets: A New Way of Making Decisions*. Eds. Robert W. Hahn and Paul C. Tetlock. Washington, DC: AEI-Brookings Joint Center for Regulatory Studies, 2006. 142-169.
- \* Hanson, Robin. “Designing Real Terrorism Futures.” *Public Choice* (forthcoming).
- \* Shachtman, Noah. “The Case for Terrorism Futures” *Wired* 30 July 2003.

## Critical Infrastructure and Control Systems Security Curriculum

### ***Session 2 – Concepts***

Objectives:

- To explore the manner in which market functioning is impaired when a high degree of uncertainty exists regarding events that are relevant to trades being conducted. The market for catastrophic risk insurance provides a good example.

Key Questions:

1. How are risks and uncertainties different?
2. What are the common types of market failures?
3. How does the presence of uncertainty affect the functioning of markets?

Readings:

- \* Chichilinsky, Graciela, and Geoffrey. M. Heal. “Managing Unknown Risks: the Future of Global Reinsurance.” Working Paper # PW-97-07. Columbia Business School, Aug. 1997.
- \* Heal, Geoffrey M., and Howard Kunreuther. “You Only Die Once: Managing Discrete Interdependent Risks.” Cambridge, MA: National Bureau of Economic Research, 2003.
- \* Dixon, Lloyd, and Robert Reville. “National Security and Private-Sector Risk Management for Terrorism.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 292-304.
- \* Macdonald, James W. “Terrorism, Insurance, and Preparedness: Connecting the Dots.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 305-337.

### ***Session 3 – Training***

Exercise:

A class exercise evidences the manner in which the existence of insurance can affect investment behavior. The activity will be drawn from the three readings below and seek to address when market solutions to security are likely to be succeed and when they are likely to fail.

Readings:

- \* Kormos, Michael, and Thomas Bowe. “Coordinated and Uncoordinated Crisis Responses by the Electric Power Industry.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 194-210.
- \* Feinstein, Jack. “Managing Reliability in Electric Power Industries.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 164-193.
- \* Roe, E., et. al. *California’s Energy Restructuring: The Challenge to Providing Service and Grid Reliability*. EPRI, Palo Alto, California Energy Commission, Sacramento, CA. rpt. no. 1007388 (Dec. 2002). ix-xix; ch. 7-9.

## Critical Infrastructure and Control Systems Security Curriculum

### *Session 4 – Actions*

#### Objectives:

To consider alternatives to pure market solutions to standards and voluntary coordination among industry participants. A class exercise focused on the exceptional challenge of simultaneously addressing aesthetic/symbolic, commercial, and security concerns in the rebuilding of the World Trade Centers will underscore the difficulties inherent to the formulation of policy in richly contested field where multiple conflicting goals are recognized. Compare and contrast with the challenge of securing CI sectors which have large sunk costs and similar complex competing concerns.

#### Key questions:

1. What are the incentives for political actors to intervene in markets where failure is not widely recognized?
2. What are the impediments to restructuring markets?
3. What are the different forms of interventions possible?

#### Readings:

- \* Epstein, Paul, and Evan Mills (eds.). “Financial Implications, Scenarios, and Solutions.” *Climate Change Futures: Health, Ecological, and Economic Dimensions*. Report of the Center for Health and the Global Environment, Harvard Medical School, 2005. 92-111.
- \* Baranoff, Dalit. “A Policy of Cooperation: the Cartelisation of American Fire Insurance, 1873–1906.” *Financial History Review* 10 (2003): 119–136.

## **Module 6: Building Trust – Public/Private Policy**

This concluding module, building on the prior lessons, will examine the pathways toward reciprocity and collective action in addressing the critical infrastructure challenge. It will focus on economic trends toward infrastructure services as a growing fraction of a high-tech competitive economy; theories for defining government, shared public/private, and private roles; sources of potential leadership to set the society on a long-term course of higher reliability and resilience of critical services.

Economic and security dependence on reliable, resilient services will continue to grow as an economy becomes more efficient, through expanded outsourcing to networked services. The threat of terrorism has now, unhappily, become a permanent threat to established societies, as population concentrations increase and terrorists have increased access to the means of destruction on a large scale. Natural disasters will continue and there is a possibility that global climate change will make some events, hurricanes and floods in particular, more severe in the future.

Finally, the growing complexity of technical networks and underlying control systems providing infrastructure services will demand more attention to and investment in means for reducing their vulnerability as their complexity and productivity grow. Open societies, characterized by a reliance on the market economy and the values and processes of a democracy, are most vulnerable to this challenge.

These facts challenge societies to find new arrangements that will increase the security of the public at a minimum cost to their efficiency and economic strength. This cannot be achieved without cooperation among competing firms, without cooperation among linked infrastructure industries, and between firms, industries, and government. The fact that CI firms must both compete and cooperate requires some level of government oversight, but the potential of disaster also calls for effective incentives to protect CI firms and industries against unpredictable events of high consequence.

This is an international as well as domestic issue. Supply chains, themselves a critical infrastructure, have become global infrastructures in themselves. Transportation, communications, and the spread of contagious disease are inherently global. Terrorist organizations are increasingly loose collaborations among groups in many nations. Thus the political obstacles, the need for new institutions, and conflicting interests arising from economics and differing risk perceptions, makes the problem even more difficult to solve.

The tools of policy will have to be imaginative. Several decades of environmental experience have demonstrated some examples of surrogate markets. Can such tools be created to deal with security externalities? One possibility is the provision of public encouragement to the insurance and reinsurance industries to build rate schedules that reward private investment in reduction of vulnerability to unlikely events. The TRIA statute, passed shortly after September 11, 2001 and renewed in the waning hours of 2005, fails to accomplish such incentives.

While these problems are daunting, the goal is surely worth pursuit: a world of societies that can make constructive provision for unavoidable acts of nature and reduce the opportunities open to would-be terrorists, and which are supported by a web of products and services that are less and less vulnerable to disasters of our own making.

## Critical Infrastructure and Control Systems Security Curriculum

### *Session 1 – Awareness*

Objectives:

Identify the tools of policy, the institutional requirements, and above all the sources of leadership that might be both effective and broadly acceptable to create a sustainable ability for societies to feel secure.

Key questions:

1. Where, within the complex of institutions (firms, cities, CI networks, nations, and multinational institutions both private and governmental), can one expect to find the institutional capacity and leadership to define the responsibilities of both private and public institutions?
2. What policies and new institutions will be required and through what political process can they come about and gain broad acceptance? Compare the competing views in the second and third readings.

Readings:

- \* Auerswald, Philip E., Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. “Leadership: Who Will Act? Integrating Public and Private Interests to Make a Safer World.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 483 –505.
- \* Bush, George W. *National Strategy for Combating Terrorism*. Washington, DC: 5 Sep. 2006.
- \* Gershman, John. “A Secure America in a Secure World.” FPIF Task Force on Terrorism. *Foreign Policy In Focus* (Sep. 2004).
- \* Lovins, Amory B., L. Hunter Lovins, and Alec Jenkins. “Achieving Resilience.” *Brittle Power: Energy Strategy for National Security*. Andover MA: Brick House Publishing Cop., 1982. 293 – 334.

### *Session 2 – Concepts*

Objectives:

- Studies of domestic and international political institutions, both intergovernmental (G-8, OECD, WTO, ITU...) and private (World Economic Forum (Davos)), academies of engineering etc., may provide some guidance as to the roots of policy reform for the mitigation of disasters.
- The politics of interest groups, including discussion of what interest groups are most important in the CIP problem, need to be understood.
- An examination of evolution of environmental protection over last 30 years may provide some important insight into what might be accomplished in the case of security from major disasters.

Key questions:

1. What kind of institutions, domestic and international, are most likely to be able to engender the trust required for effective collaboration?
2. What conflicting interests in the international community are likely to raise the most difficult political problems domestically, and how might they be ameliorated?
3. What can we learn from the experience of environmental externalities that might inform the institutional arrangements required for CIP?

## Critical Infrastructure and Control Systems Security Curriculum

### Readings:

\* Michel-Kerjan, Erwann, and Nathalie de Marcellis-Warin. "Public-Private Programs for Covering Extreme Events: The Impact of Information Distribution on Risk Sharing." *Asia-Pacific Journal of Risk and Insurance* 1.1 (2006):21-49.

### **Session 3 – Training**

#### Objectives:

All-hazards disaster management is not only important to all nations, but its attainment is essentially a global problem. The objective in this session is an overview of the CIP situation in 20 countries, including the United States, learning how different and how effective their approaches are, and considering the merits of collaboration among them.

#### Exercise:

Teams of three students with different disciplinary backgrounds will read the U.S. case in the reading (pp. 311-342), then look through Appendix 1 and select a country whose CIP program looks to you well conceived. Prepare a discussion of the two cases you have selected (United States and one other). Teams may also refer to the material on international institutions.

#### Key questions:

1. How does the U.S. approach to CIP compare with that of other liberal market democracies?
2. To what extent may formal arrangements among nations contribute to the safety of each?
3. Through what kinds of institutions might those arrangements best be formulated?

#### Readings:

\* Abele-Wigert, Isabelle, and Myriam Dunn. *International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations*. Vol. 1. Zurich: Center for Security Studies, ETH, 2006.

### **Session 4 – Actions**

#### Objectives:

Policies that cannot be implemented for economic or political reasons are not only useless but often get in the way of serious negotiations on more practical plans, even if agreement is difficult to achieve. Leadership must be prepared to take some risks, to be held accountable and to build long-term support for sustainable results is required.

#### Key questions:

1. Where will leadership come from, individuals or institutions, private or public sectors, domestic or international organizations?
2. Under what circumstances can U.S. government leaders and institutions be expected to take the lead?

## Critical Infrastructure and Control Systems Security Curriculum

3. Are the economic arguments for expanded private investments in risk reduction viable and sustainable, even in the absence of serious threats from catastrophic terrorism? If so, how can the debate be shifted to these longer term economic and social goals?

### Readings:

- \* Carter, Ashton. "The Architecture of Government in the Face of Terrorism." *International Security* 26.3 (Winter 2001/02): 5–23.
- \* Farmer, Richard D. "Homeland Security and the Private Sector." Washington, DC: Congressional Budget Office, Dec. 2004.
- \* Committee on Science and Technology in Countering Terrorism, National Research Council. "Essential Partners in a National Strategy: States and Cities, Industry, and Universities." *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academies Press, 2002. 357-371.

**Appendix A**  
**Modular Design**

## Appendix A

### Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>1. Vulnerability of Critical Infrastructures</b>				
Role of Critical Infrastructure (CI) in the economy, identification of risks in prior White House studies, problem of private sector incentives in the face of security externalities, government assumption that markets are sufficient, the all-hazards, all-scales approach (firm, industry, cross-industry), difficulty of defining risks, and policy problem of defining accountability between government and private sector.				
<b>Objective</b>	<p>To understand:</p> <ul style="list-style-type: none"> <li>* History of federal concern over CI vulnerability to terrorism</li> <li>* Official counts of number of CIs</li> <li>* Limitations of markets to account for vulnerabilities</li> <li>* Economic role of CI</li> <li>* Unresolved federal/private division of accountability for CI protection</li> <li>* Creation of the Department of Homeland Security (DHS)</li> </ul> <p>To open discussion concerning</p> <ul style="list-style-type: none"> <li>* The necessity of an all-hazards approach</li> <li>* Adequacy of approach taken in the National Infrastructure Protection Plan</li> </ul>	<p>To understand fundamental concepts of security economics:</p> <ul style="list-style-type: none"> <li>* Security externalities and endogenous vulnerabilities</li> <li>* Loss of resilience as a consequence of maximized efficiency</li> </ul> <p>The concepts of resiliency, robustness, and reliability</p> <p>To explore:</p> <ul style="list-style-type: none"> <li>* Political/economic context within which infrastructure services must both compete and cooperate</li> <li>* The possibility of public policies based on collaborative governance</li> </ul>	<p>To develop a practical appreciation for the tradeoffs inherent in setting priorities for investments to reduce CI vulnerabilities.</p>	<p>To develop prospective view of the issues that must be confronted in reducing infrastructure vulnerabilities:</p> <ul style="list-style-type: none"> <li>* Technical sources of vulnerability</li> <li>* Assessing vulnerabilities and risks</li> <li>* Managing high-reliability, resilient enterprises</li> <li>* Complications from interdependence of multiple firms in same industry and intra-dependence of multiple CIs</li> <li>* Understanding the important role of information technology in general and control systems in particular.</li> <li>* The importance of both management and technology issues to be addressed together.</li> <li>* Creating markets to induce private investment</li> <li>* Finding leadership to build public-private cooperation</li> </ul>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>Questions (max 3 per session)</b>	<p>1. How has the federal government changed its role with relation to CI industries' vulnerability to terrorism?</p> <p>2. What are the benefits and drawbacks of an all-hazards approach to federal disaster policy?</p>	<p>1. Under what circumstances do firms in a service industry both compete and cooperate effectively? Is resilience always a casualty of increasing efficiency?</p> <p>2. What factors govern a firm's willingness to invest in vulnerability reduction when facing very low risks of serious consequence?</p> <p>3. What is the political-economic context for seeking government-industry collaboration in creating and executing an effective Critical Infrastructure Protection (CIP) policy?</p>		<p>1. How well structured is the U.S. government for addressing those issues (such as CIP) where information technology is especially important?</p> <p>2. What are the resources available in industry and in government and how do they compare and relate?</p> <p>3. What do the appropriate policies for two classes of disaster have in common: (a) disasters caused by either terrorists or nature and (b) disasters caused by some combination of poor management, wrong engineering, and regulatory environments inappropriate to high resilience?</p>
<b>Case(s) and/or motivating exercise(s)</b>			<p><i>Exercise:</i> Create mixed discipline teams of students. Ask them to consider the example of the electrical energy industry, a critical infrastructure service whose reliability and resilience are threatened by expanding government deregulation, and where management goals diverge from promoting security and the reduction of vulnerability in an environment where risk cannot be quantified. Discuss how corporate executives who feel strong competitive pressure would make decisions about such</p>	

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
			investments, including how they might go about estimating risks, costs, and benefits and how they might be influenced by decisions of their competitors (who may face same vulnerability, but different risks).	
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	<ul style="list-style-type: none"> <li>* U.S. Department of Homeland Security. "Executive Summary." <i>National Infrastructure Protection Plan</i>.</li> <li>* Flynn, Stephen E. "The Neglected Home Front." <i>Foreign Affairs</i>.</li> <li>* Homer-Dixon, Thomas. "The Rise of Complex Terrorism." <i>Foreign Policy</i>.</li> <li>* Branscomb, Lewis M. "A Nation Forewarned: Vulnerability of Critical Infrastructure in the 21st Century." <i>Seeds of Disaster, Roots of Response</i>.</li> <li>* Lovins, Amory B. and L. Hunter Lovins. "National Energy Insecurity." <i>Brittle Power: Energy Strategy for National Security</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Auerswald, Philip, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan. "Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge." <i>Seeds of Disaster, Roots of Response</i>.</li> <li>* Longstaff, Pat. <i>Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology</i>. 1-42.</li> <li>* Donahue, John D. "On Collaborative Governance."</li> <li>* Lopez, Brian. "Evolution of Vulnerability Assessment Methods." <i>Seeds of Disaster, Roots of Response</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Committee on Science and Technology in Countering Terrorism, National Research Council. "Energy Systems." <i>Making the Nation Safer</i>.</li> <li>* Nevius, David R. and Ellen P. Vanco. "Ensuring a Reliable North American Electric System in a Competitive Market Place."</li> </ul>	<ul style="list-style-type: none"> <li>* Committee on Science and Technology in Countering Terrorism, National Research Council. "Executive Summary." <i>Making the Nation Safer</i>.</li> <li>* Committee on Science and Technology in Countering Terrorism, National Research Council. "Information Technologies." <i>Making the Nation Safer</i>.</li> </ul>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>2. Engineering Approaches</b>				
The opportunities and limits of engineered solution to the CI challenge, with a primer on technologies employed, their historic context, and current key issues. Principal emphasis is on control systems, but other modules also examine other scenarios.				
<b>Objective</b>	To understand: * The key technologies underlying critical control infrastructures in various industries in the U.S. * Design considerations for these systems in light of threats of natural or man-made catastrophic events	To understand: * How Supervisory Control and Data Acquisition (SCADA) and other control systems are evolving as a result of changes in computer and network technology * The economic drivers behind these changes * How these changes positively and negatively impact the vulnerability of these systems	To understand: * That operator training in control systems is as important as the system technology To generate: * Dialog about wide-scale systemic risks generated by a high-altitude electromagnetic pulse (HEMP) attack	To explore: * How technical tradeoffs are made in industry * How CIP fits into managerial perspective
<b>Questions (max 3 per session)</b>	1. What are the key technologies that underlie CI control in the U.S.? 2. What are SCADA systems and why were they developed? 3. What are the key vulnerabilities of these technologies in light of the range of threats from all hazards?	1. How have computerized systems expanded their role in various CI providers? 2. What are the changes in the off the shelf technology, hardware, software, and network and how have these changed the capabilities and vulnerabilities of SCADA systems? 3. How have the risks of intrusion or failure increased as a result of network connectivity and standards?	1. What were the primary causes of failure at Three Mile Island? Why were these unlikely to occur in the nuclear Navy? 2. What is an EMP and why is it such a major risk? 3. What were the technical and organizational causes of the NE Blackout of 2003?	1. How can non-technical managers evaluate technical risk, comparing the variety of hazards such as natural disasters, terrorism, and human error? 2. What is right and wrong with the current models of economic analysis? 3. How can the increased cost of CIP be justified and managed?

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>Case(s) and/or motivating exercise(s)</b>	Basic SCADA system design, including technology building blocks (build a SCADA for a electric generating plant on paper at a block level)	Comparisons of historic proprietary SCADA environments, moving to industry standards, and new NIST secure standards	Operations at Three Mile Island compared with a nuclear sub; HEMP threat	Three Mile Island Managerial Decisions Capital Investment Strategy, Risk Reward Exercise
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	<ul style="list-style-type: none"> <li>* Apt, J., L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic. "Electrical Blackouts: A Systemic Problem."</li> <li>* U.S. General Accounting Office. "Critical Infrastructure Protection: Challenge and Efforts to Secure Control Systems."</li> <li>* Shaw, William. <i>Cybersecurity for SCADA Systems.</i></li> </ul>	<ul style="list-style-type: none"> <li>* Nash, Troy. "Backdoors and Holes in Network Perimeters."</li> <li>* Nash, Tony. "An Undirected Attack Against Critical Infrastructure."</li> <li>* U.S. House Committee on Governmental Reform. <i>Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure.</i></li> <li>* Permann, May Robin, and Kenneth Rohde. "Cyber Assessment Methods." <i>InTech.</i></li> </ul>	<ul style="list-style-type: none"> <li>* Nuclear Regulatory Commission. <i>Three Mile Island: A Report to the Commissioners and to the Public.</i></li> <li>* U.S.-Canada Power System Outage Task Force. <i>Final Report on the August 14, 2003 Blackout in the U.S. and Canada.</i></li> <li>* Sweet, William. "The Blackout of 2003."</li> <li>* Foster, et al. "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack"</li> <li>* <i>Testimony of Vice Admiral Hyman George Rickover, Naval Nuclear Propulsion Program--1972-73.</i></li> </ul>	<ul style="list-style-type: none"> <li>* Nuclear Regulatory Commission. <i>Three Mile Island: A Report to the Commissioners and to the Public.</i></li> <li>* Schneier, Bruce. "Non-Security Considerations in Security Decisions."</li> </ul>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>3. Managing Organizations and Risk</b>				
An examination of the opportunities and limits of management and organizational practices as tools to address CI challenges within the enterprise. Contrasting strategies to achieve assured high operations reliability focused on flexibility and responding to the unexpected, versus defining quantitatively the risks and means to reduce them individually.				
<b>Objective</b>	<p>To understand:</p> <ul style="list-style-type: none"> <li>* The special properties and dynamics of large technical systems</li> <li>* The debates about “normal accidents” (Perrow) and highly reliable organizations (HROs)</li> </ul>	<p>To understand fundamental concepts fundamental to the study of organizations including:</p> <ul style="list-style-type: none"> <li>* Agency and accountability</li> <li>* The difference between organizational structure and communications structure</li> <li>* Anticipation and resilience</li> <li>* Tightly coupled, hierarchical and linear-type systems</li> <li>* Loosely-coupled, non-hierarchical, non-linear systems</li> <li>* Highly reliable organization theory</li> <li>* Risk migration</li> <li>* System design and reliability professional</li> <li>* Organizational mindfulness</li> </ul>	<p>To develop a better understanding of the key concepts in the first two sessions through a tabletop simulation. The exercise will result in increased awareness in each group of the perspective, interests and concerns of the other groups, to encourage better designs, both for normal operations as well as during extreme events such as widespread blackouts or a terrorist attack.</p>	<p>To develop a prospective view of the issues that must be confronted with respect to management of complex and interdependent technical systems facing turbulent environments under the most stringent constraints of reliable operations.</p> <p>To discuss the tradeoffs and challenges of reconciling security, reliability, and efficiency of critical infrastructure systems in democratic societies.</p>
<b>Questions (max 3 per session)</b>	<ol style="list-style-type: none"> <li>1. What are the technical, organizational, and social implications of attempting to reduce failure to zero? What is the economic cost of doing so?</li> <li>2. In complex technological and organizational settings, where powerful, risky, or essential systems are being operated in dynamic and/or turbulent environments, how can risk assessment</li> </ol>	<ol style="list-style-type: none"> <li>1. After outlining the main characteristics of highly reliable or "mindful" organizations, assess to what extent they exist in specific critical infrastructure or homeland security organizations. What are the challenges to managers of adopting structures or practices that would result in improved reliability or mindfulness?</li> </ol>	<p>Question in this session will flow from those in the previous sessions, and will focus on the issues that arise in the course of the exercise.</p>	<ol style="list-style-type: none"> <li>1. How can a policy to reduce CI vulnerability at the national level be designed to take into account the impacts of management practice and organizational structure on reliability?</li> <li>2. How can the concept of resilience, either at the organizational, community, or national levels most effectively inform policy for homeland security?</li> </ol>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
	<p>techniques best be used? Do they have limitations? If so, how should such limitations be addressed by organization managers?</p> <p>3. If failure is unacceptable in managing such complex and critical systems and if trial and error learning is not useful, what tools, perspectives, and methods can managers use to minimize risks to their systems and the society that relies on them? How applicable are traditional management techniques in such situations? How would your answer have to change to take suicide terrorist actions into account?</p>	<p>2. Most critical technical systems (such as the SCADA systems discussed in Module 2) are designed and operated by different people, working with different assumptions, and with different objectives. Some systems are so complex that seemingly no single person really understands them. How do risks, design flaws, or vulnerabilities get identified and corrected in such situations? What impediments are there to making improvements?</p> <p>3. What are the external political requirements for operating highly reliable, mindful, or essential systems? How can these conditions be sustained over long periods? What might happen if these conditions change?</p>		<p>3. How do economic incentives for efficiency conflict with the need for reliability and security?</p>
<b>Case(s), and or motivating exercise(s)</b>	<ul style="list-style-type: none"> <li>* Crash of the Space Shuttle Columbia</li> <li>* Operations on aircraft carriers</li> </ul>		<p>Create three teams (or depending on the size of the group, two sets of teams). One team will be “Systems Designers,” the second will be “Operators,” and the third, “Attackers.” These three teams will engage in an iterative table-top simulation of the dynamics of systems design, systems operation and terrorist or other attack, with special emphasis on system reliability during</p>	

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
			extreme events or stress.	
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	<ul style="list-style-type: none"> <li>* La Porte, Todd R. "Challenges of Assuring High Reliability When Facing Suicide Terrorism." <i>Seeds of Disaster, Roots of Response</i>.</li> <li>* Weick, Karl E., Kathleen M. Sutcliffe, Robert E. Quinn. <i>Managing the Unexpected: Assuring High Performance in an Age of Complexity</i>. 1-84.</li> </ul>	<ul style="list-style-type: none"> <li>* La Porte, Todd M. "Organizational Strategies for Complex Systems Resilience, Reliability, and Adaptation." <i>Seeds of Disaster, Roots of Response</i>.</li> <li>* Perrow, Charles. "Complexity, Coupling and Catastrophe" and "Living with High Risk Systems." <i>Normal Accidents: Living with High-Risk Technologies</i>.</li> <li>* Wildavsky, Aaron. "Anticipation and Resilience" and "The Secret of Safety Lies in Danger." <i>Searching for Safety</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Schulman, P.R., E. Roe, M. van Eeten, and M. de Bruijne. "High Reliability and the Management of Critical Infrastructures." <i>Journal of Contingencies and Crisis Management</i>.</li> <li>* Roe, E., et. al. <i>California' Energy Restructuring: The Challenge to Providing Service and Grid Reliability</i>. (Note: Entire report).</li> <li>* U.S.-Canada Power System Outage Task Force. <i>Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Perrow, Charles. "Organizing to Reduce the Vulnerabilities of Complexity." <i>Journal of Contingencies and Crisis Management</i>.</li> <li>* Rochlin, Gene. <i>Trapped in the Net: The Unanticipated Consequences of Computerization</i>. See especially Chapters 10-12.</li> <li>* U.S. National Aeronautics and Space Administration. <i>Final Report of the Columbia Accident Investigation Board</i>. Chapters 5-8, 11.</li> </ul>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>4. Securing Networks of Enterprises</b>				
The challenges of infrastructure interdependencies in multi-firm industries and the relationship to the dependencies and organizational politics within firms, as discussed in Module 3. Includes examination of the problems of accountability; inefficiencies from vertical integration to reduce risk of interdependence; recognition of global interdependencies (in supply chains, for example).				
<b>Objective</b>	To explore: * The interdependency of CI across players in a supply or value chain * How "localized" failures move through the system	To understand: * The concept of intra-organizational and inter-organizational networks * How economic optimization and impacts vulnerability * System economics given certain assumptions (e.g., fuel costs)	To understand: * Interdependencies of control systems * Inter-organizational impacts of disruption	To examine: * The economics of the CIP issues * Who benefits and who bears the risk within the current system * How managers consider risk
<b>Questions (max 3 per session)</b>	1. What has led us to create these complex, geographically distributed, and vulnerable systems? 2. How have these created a more flexible and global business environment? 3. What are the risks associated with this business architecture?	1. Explain the concepts of optimization and hyper criticality. 2. What are the risks in the current extended supply chain systems? 3. How might a failure in one component propagate and how might it be minimized?		1. Why might investments in CIP often be a lower priority than current profits? 2. To what extent can critical infrastructure and control systems security investments be justified on the basis of interdependency risks? 3. What are the incentives that might be changed to alter managerial behavior? 4. What is the market role and the role of regulation?
<b>Case(s) and/or motivating exercise(s)</b>	Wal-Mart The Northeast Power Blackout	NE Power Grid NW Pipeline SCADA	The instructor will divide the group into teams of three or four and will provide a basic template of the PERT chart with three corporate parties in a supply chain and within each of four system paths. One of these paths will cause major failures in supply and the others have redundancy. The students will complete these charts and operate the	Telco Industry

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
			models under failure scenarios describing the resulting impacts of up stream failures and recommending approaches to robustness. Also the instructor will guide the student in a discussion on economic tradeoffs in robustness.	
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	<ul style="list-style-type: none"> <li>* Kinsey, Jean. "A Faster, Leaner, Supply Chain: New Uses of Information Technology." <i>American Journal of Agricultural Economics</i>.</li> <li>* Amin, M. "National Infrastructures as Complex Interactive Networks." <i>Automation, Control, and Complexity: An Integrated Approach</i>.</li> <li>* U.S.-Canada Power System Outage Task Force. <i>Final Report on the August 14, 2003 Blackout in the U.S. and Canada</i>.</li> <li>*Sheffi, Yossi. <i>The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage</i>. Chapters 7 and 16.</li> </ul>	<ul style="list-style-type: none"> <li>* Carlson, J.M., and John Doyle. "Complexity and Robustness." <i>Proceedings of the National Academy of Sciences of the United States of America</i>.</li> <li>* U.S. Department of Energy. <i>21 Steps to Improve Cyber Security of SCADA Networks</i>.</li> <li>* U.S. House Committee on Governmental Reform. <i>Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure</i>.</li> <li>* St Sauver, Joe. "SCADA Security and Critical Infrastructure."</li> </ul>	<ul style="list-style-type: none"> <li>* Nishiguchi, Toshihiro, and Aiexandre Beaudet. "Self-Organization and Clustered Control in the Toyota Group: Lessons from the Akin Fire."</li> <li>* Lawler, Andrew. "Faster, Cheaper, Better on Trial." <i>Science</i>.</li> <li>* Chatfield, Carl, and Timothy Johnson. <i>Microsoft Office Project 2003: Step by Step</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Greenstein, Shane M. "The Economic Geography of Internet Infrastructure in the United States."</li> <li>* Gordon, Lawrence A., Martin A. Loeb, and William Lucyshyn. "Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets."</li> <li>* Garcia, Alfredo, and Barry Horowitz. "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy."</li> <li>* Peterson. Dale, Matt Franz, and Landon Lewis. <i>SCADA Security</i>.</li> </ul>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>5. Creating Markets</b>				
Limits of market-based approaches to addressing critical infrastructure challenges and policy opportunities for overcoming these limitations. Emphasis on policy tools available to government, such as incentives for insurance and re-insurance industries, defined legal vulnerabilities, cost shared investments in R&D, and validation.				
<b>Objective</b>	To understand: * How markets can be used to aggregate information and coordinate actions * What prerequisites exist for market functioning * The policy challenges posed by poor quality public information	To understand fundamental economic concepts relevant to CI including: * Markets and market failure * Risk and uncertainty * Externalities * Skewed outcome distributions	To develop intuition regarding inter-dependent security and market function	To consider alternatives to pure market solutions to standards and voluntary coordination among industry participants.
<b>Questions (max 3 per session)</b>	1. How does terrorism challenge the role of markets in aggregating information? 2. What institutions are necessary for market functioning?	1. How are risks and uncertainties different? 2. What are the common types of market failures? 3. How does the presence of uncertainty affect the functioning of markets?	1. Under what conditions are market solutions to security challenges ideal? 2. Under what conditions are market solutions to security likely to fail? 3. What are the barriers to interdependent security?	1. What are the incentives for political actors to intervene in markets where failure is not widely recognized? 2. What are the impediments to restructuring markets? 3. What are the different forms of interventions possible?
<b>Case(s) and/or motivating exercise(s)</b>	* Insurance for climate change * The DARPA market for Terrorism Risk		A class exercise evidences the manner in which the existence of insurance can affect investment behavior. The activity will be drawn from the three readings below and seek to address when market solutions to security are likely to succeed and when they are likely to fail.	
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	* Hahn, Robert W., and Paul C. Tetlock. "Introduction to Information Markets." <i>Information Markets: A New Way of Making Decisions.</i> * Berg, Joyce E., and Thomas A. Rietz. "The Iowa	* Chichilinsky, Graciela. and Geoffrey. M. Heal. "Managing Unknown Risks: the Future of Global Reinsurance." * Heal, Geoffrey M., and Howard Kunreuther. "You Only Die Once: Managing	* Kormos, Michael, and Thomas Bowe. "Coordinated and Uncoordinated Crisis Responses by the Electric Power Industry." <i>Seeds of Disaster, Roots of Response.</i> * Feinstein, Jack. "Managing	* Epstein, Paul, and Evan Mills (eds.). "Financial Implications, Scenarios, and Solutions." <i>Climate Change Futures: Health, Ecological, and Economic Dimensions.</i> * Baranoff, Dalit. "A Policy of

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
	<p>Electronic Markets: Stylized Facts and Open Issues.”  <i>Information Markets: A New Way of Making Decisions.</i>            * Hanson, Robin. “Designing Real Terrorism Futures.”  <i>Public Choice.</i>            * Shachtman, Noah. “The Case for Terrorism Futures.”</p>	<p>Discrete Interdependent Risks.”            * Dixon, Lloyd, and Robert Reville. “National Security and Private-Sector Risk Management for Terrorism.”  <i>Seeds of Disaster, Roots of Response.</i>            * Macdonald, James W. “Terrorism, Insurance, and Preparedness: Connecting the Dots.” <i>Seeds of Disaster, Roots of Response.</i></p>	<p>Reliability in Electric Power Industries.” <i>Seeds of Disaster, Roots of Response.</i>            * Roe, E., et. al. <i>California’s Energy Restructuring: The Challenge to Providing Service and Grid Reliability.</i>ix-xix; Chapters 7-9.</p>	<p>Cooperation: the Cartelisation of American Fire Insurance, 1873–1906.”  <i>Financial History Review.</i></p>

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
<b>6. Building Trust – Public/Private Policy</b>				
Pathways toward reciprocity and collective action in addressing the CI challenge. Focus on economic trends toward infrastructure services as a growing fraction of a high-tech competitive economy; theories for defining government, shared public/private and private roles; sources of potential leadership to set the society on a long-term course of higher reliability and resilience of critical services.				
<b>Objective</b>	Identify the tools of policy, the institutional requirements, and above all the sources of leadership that might be both effective and broadly acceptable to create a sustainable ability for societies to feel secure.	To consider: * Possible sources of policy reform for the mitigation of disasters * The politics and role of interest groups in CIP.	To understand different national and international approaches to CIP and consider their merits.	To understand the need for and consider sources of leadership in CIP.
<b>Questions (max 3 per session)</b>	1. Where, within the complex of institutions (firms, cities, CI networks, nations, and multinational institutions both private and governmental) can one expect to find the institutional capacity and leadership to define the responsibilities of both private and public institutions? 2. What policies and new institutions will be required and through what political process can they come about and gain broad acceptance? Compare the competing views in the second and third readings.	1. What kind of institutions, domestic and international, are most likely to be able to engender the trust required for effective collaboration? 2. What conflicting interests in the international community are likely to raise the most difficult political problems domestically and how might they be ameliorated? 3. What can we learn from the experience of environmental externalities that might inform the institutional arrangements required for CIP?	1. How does the U.S. approach to CIP compare with that of other market economy democracies? 2. To what extent may formal arrangements among the nations contribute to the safety of each? 3. Through what kinds of institutions might those arrangements best be formulated?	1. Where will this leadership come from: individuals or institutions, private or public sectors, domestic or international organizations? 2. Under what circumstances can the U.S. government leaders and institutions be expected to take the lead? 3. Are the economic arguments for expanded private investments in vulnerability reduction viable and sustainable, even in the absence of serious threats from catastrophic terrorism? If so, how can the debate be shifted to these longer-term economic and social goals?
<b>Case(s) and/or motivating exercise(s)</b>			Teams of three students with different disciplinary backgrounds will read the U.S. case in the reading (pp. 311-342), then look through Appendix 1 and select a country whose CIP program looks to you well-conceived.	

Critical Infrastructure and Control Systems Security Curriculum  
Appendix A – Modular Design

	<b>Session 1 Awareness</b> <i>Issue Setting, Overview</i>	<b>Session 2 Concepts</b> <i>Pedagogy</i>	<b>Session 3 Training</b> <i>Cases and Exercises</i>	<b>Session 4 Actions</b> <i>Take-aways</i>
			Prepare a discussion of the two cases you have selected (U.S. and one other). Teams may also make reference to the material on international institutions.	
<b>Readings (max 3 per session)</b> <i>Please note, full citations can be found in Appendix B</i>	<ul style="list-style-type: none"> <li>* Auerswald, Philip E., Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. "Leadership: Who Will Act? Integrating Public and Private Interests to Make a Safer World." <i>Seeds of Disaster, Roots of Response</i>.</li> <li>* Bush, George W. <i>National Strategy for Combating Terrorism</i>.</li> <li>* Gershman, John. "A Secure America in a Secure World." FPIF Task Force on Terrorism. <i>Foreign Policy In Focus</i>.</li> <li>* Lovins, Amory B., L. Hunter Lovins, and Alec Jenkins. "Achieving Resilience." <i>Brittle Power: Energy Strategy for National Security</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Michel-Kerjan, Erwann, and Nathalie de Marcellis-Warin. "Public-Private Programs for Covering Extreme Events: The Impact of Information Distribution on Risk Sharing." <i>Asia-Pacific Journal of Risk and Insurance</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Abele-Wigert, Isabelle, and Myriam Dunn. <i>International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations</i>.</li> </ul>	<ul style="list-style-type: none"> <li>* Carter, Ashton. "The Architecture of Government in the Face of Terrorism." <i>International Security</i>.</li> <li>* Farmer, Richard D. "Homeland Security and the Private Sector."</li> <li>* Committee on Science and Technology in Countering Terrorism, National Research Council. "Essential Partners in a National Strategy: States and Cities, Industry, and Universities." <i>Making the Nation Safer</i>.</li> </ul>

**Appendix B**  
**Annotated Bibliography**

## Appendix B

### Annotated Bibliography

#### Module 1: Vulnerability of Critical Infrastructures

##### 1.1

- 1.1.1. United States. Department of Homeland Security. “Executive Summary.” *National Infrastructure Protection Plan*. Washington, DC: 2006. 15-20. Available Online: <[http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIPP\\_Plan\\_ExecSumm.pdf](http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIPP_Plan_ExecSumm.pdf)>.

This official government plan, led by DHS and signed onto by most cabinet members, describes in great detail the roles and goals of all federal agencies in CIP, but says surprisingly little about the private sector and in general says little about implementation (resources, timetables, accountability, progress monitoring). It speaks extensively about partnerships, but not about how they are to be achieved. The full document can be found in Appendix C.

- 1.1.2. Flynn, Stephen E. “The Neglected Home Front.” *Foreign Affairs* 83.1 (2004): 20–33. Available Online: <[www.foreignaffairs.org](http://www.foreignaffairs.org)>.

This thoughtful paper puts the homeland security issues, especially the vulnerability of CIs in the context of the broader issues of terrorism threats and defenses. It is critical of what the U.S. government has so far achieved in this area.

- 1.1.3. Homer-Dixon, Thomas. “The Rise of Complex Terrorism.” *Foreign Policy* 128 (Jan./Feb. 2002): 52-62. Available Online: <[www.foreignpolicy.com](http://www.foreignpolicy.com)>.

An excellent paper on the complexities of terrorism threats emphasizing the interdependent dimensions of both threats and solutions.

- 1.1.4. Branscomb, Lewis M. “A Nation Forewarned: Vulnerability of Critical Infrastructure in the 21<sup>st</sup> Century.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 19-25.

A succinct introduction to the context of the political notion of a “war on terror,” the pre-September 11, 2001 run up to the current situation, the problem of adequate tools for evaluating vulnerabilities and risks, and the necessity of a sustainable national effort to make a high-tech economy both safe and secure from all kinds of disasters, not just terrorism threats.

- 1.1.5. Lovins, Amory B. and L. Hunter Lovins. “National Energy Insecurity.” *Brittle Power: Energy Strategy for National Security*. Andover MA: Brick House Publishing Cop., 1982. 1- 10.

The first chapter of this book published a quarter century ago may entice you to read more of it (see supplementary readings listed below). The authors have a long history of advocacy of green technology, but in this book they focus on the risks, including risks of terrorism from centralized, over-scaled technologies. This book provides an interesting perspective that, in the wake of much greater consequences in disasters, is worth revisiting.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

## 1.2

- 1.2.1. Donahue, John D. “On Collaborative Governance.” CSRI Working Paper Series #2. Kennedy School of Government, Harvard University, Feb. 2004. Available Online: <[http://www.ksg.harvard.edu/m-rcbg/CSRI/publications/workingpaper\\_2\\_donahue.pdf](http://www.ksg.harvard.edu/m-rcbg/CSRI/publications/workingpaper_2_donahue.pdf)>.

If the only path to improving the robustness and resilience of CIs requires much more effective trust and cooperation between public and private sectors, some form of collaborative governance will be needed. This introduces the concept of collaborative government, its strengths, weaknesses, and prospects for effectiveness.

- 1.2.2. Longstaff, Pat. Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology. Program on Information Resource Policy, Harvard University, 2005. 1-42. Available Online: <[www.pirp.harvard.edu/publications/pdf-blurb.asp?id=606](http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=606)>.

This monograph introduces the concept of resilience in the context of disasters. The first 42 pages introduce the idea, but a skim through the rest of the monograph will be rewarding.

- 1.2.3. Lopez, Brian. “Evolution of Vulnerability Assessment Methods.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 51-68.

Lopez provides an introduction to the challenges and approaches of assessing the vulnerability of CI and key assets. This chapter offers a discussion of governmental action in gauging vulnerability over the course of the past eight years. Varying approaches to understanding the interrelationship between the three components that help define risk are considered: threats, vulnerabilities, and consequences.

- 1.2.4. Auerswald, Philip, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, “Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 3-12.

This introductory chapter to the book describes important economic concepts required in this course. It explores the way the quest for efficiency comes at the expense of resilience, discusses a new view of security externalities, explores the effectiveness of shared governance, searches for policy proxies for market forces and a clear allocation of accountability, and creates robust policies and institutions through which they can be implemented.

## 1.3

- 1.3.1. Committee on Science and Technology in Countering Terrorism, National Research Council. “Energy Systems.” *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academies Press, 2002. 177 – 209. Available Online: <<http://newton.nap.edu/catalog/10415.html>>.

This analysis summarizes the vulnerabilities in the energy industry and makes recommendations on needed R&D to reduce those vulnerabilities. This course uses control systems as the central technology on which firms in many industries depend for efficiency and which often exacts a price in robustness and resilience. One main example is energy systems.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

- 1.3.2. Nevius, David R. and Ellen P. Vanco. “Ensuring a Reliable North American Electric System in a Competitive Market Place.” Prepared for the U.S.-Canada Power System Outage Task Force. 15 Aug. 2005. Available Online: <[ftp://www.nerc.com/pub/sys/all\\_updl/docs/blackout/NERC\\_recommendation\\_12-technical\\_edits.pdf](ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/NERC_recommendation_12-technical_edits.pdf)>.

This input to the major study of the causes of the 2003 Northeast power blackout frames the problem in a succinct way and summarizes recommendations.

## 1.4

- 1.4.1. Committee on Science and Technology in Countering Terrorism, National Research Council. “Executive Summary.” *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press, 2002. 1-24. Available Online: <[http://books.nap.edu/execsumm\\_pdf/10415.pdf](http://books.nap.edu/execsumm_pdf/10415.pdf)>.

This document outlines the big picture: the key technical perspectives on terrorism vulnerabilities combined with the context in which society will have to address these problems. The technical chapters of this book had a substantial influence on the DHS science and technology (S&T) strategy, but its concerns about the context, summarized in this Executive Summary, have not been acted on to the same extent.

- 1.4.2. Committee on Science and Technology in Countering Terrorism, National Research Council. “Information Technologies,” *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press, 2002. Available Online: <<http://newton.nap.edu/catalog/10415.html>>.

Control systems depend almost universally now on computers, software, and digital networks. The vulnerabilities of those technologies are summarized in this expert analysis. These two readings serve as a base line for the next module.

### Module 1 Supplementary Readings:

- \* Longstaff, Pat. Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters, and Complex Technology. Program on Information Resource Policy, Harvard University, 2005. Available Online: <[www.pirp.harvard.edu/publications/pdf-blurb.asp?id=606](http://www.pirp.harvard.edu/publications/pdf-blurb.asp?id=606)>.

This monograph is a valuable and accessible exploration of the terms so often used imprecisely in connection with issues of security in the face of disasters. It is recommended that this entire monograph be read selectively.

- \* Moteff, John, Claudia Copeland, and John Fischer. “Critical Infrastructure: What Makes an Infrastructure Critical?” CRS Report RL301556. 2003. Available Online: <[www.fas.org/irp/crs/RL31556.pdf](http://www.fas.org/irp/crs/RL31556.pdf)>.

A short introduction into the expansion of CI definitions and the challenges such definitions pose for policy makers. The key questions considered are: How have CI definitions expanded? Why is this expansion of interest/concern? Is there a better way to define the scope of CI?

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

- \* Moteff, John D. “Critical Infrastructure: Background, Policy, and Implementation.” CRS Report RL30153. 2006. Available Online: <[www.fas.org/sgp/crs/homsec/RL30153.pdf](http://www.fas.org/sgp/crs/homsec/RL30153.pdf)>.

This recent report from the Congressional Research Service provides an overview of public interest in CI, mostly focusing on current period (beginning in 1996) but also some additional material stretching back further. The report offers a discussion of key topics, legislative history, and institutional responsibilities. The three main themes covered are: the allocation of resources based on risk, information sharing, and regulation.

- \* Lopez, Brian. “Critical Infrastructure Protection in the United States Since 1993.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 37-50.

An introduction into the history of domestic concern with CIP.

- \* Flynn, Stephen. *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*. New York: HarperCollins, 2004.

Building on the short article assigned as required reading, Flynn provides a forceful argument demonstrating the inadequacy of current policies designed to protect CI.

- \* Lovins, AB, & Lovins, LH. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House, 1982.

Based on a report commissioned by the Defense Civil Preparedness Agency, this book outlines the ways in which U.S. energy is brittle, prone to possible disruption through intentional and unintentional acts. The book considers natural events, technological/complex system failure, over-reliance on imports, and military and terrorist attacks. Most importantly, the book offers an early consideration of the differences between intentional and unintentional disruptions, strategies of design, economic trends (increased centralization of particular functions leading to localized failures with global or national significance), and discussion of ways to insure greater security through diversification, redundancy, decentralization, and resiliency in the face of the inevitability of surprise. The book anticipates much of the discussions of the past decade, sketching the problems well and offering solutions that are still relevant.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

**Module 2: Engineering Approaches**

**2.1**

- 2.1.1. Apt, J., L. B. Lave, S. Talukdar, M. G. Morgan, and M. Ilic. “Electrical Blackouts: A Systemic Problem.” *Issues in Science and Technology* 20.4 (2004): 55–61. Available Online: <[http://wpweb2k.gsia.cmu.edu/ceic/pdfs\\_other/Electrical\\_Blackouts.pdf](http://wpweb2k.gsia.cmu.edu/ceic/pdfs_other/Electrical_Blackouts.pdf)>.

This report provides a good overview of the causes of blackouts, focusing on infrastructure and inter-organizational complexities. It illustrates the problems of control systems operating CI and the complex environment within which many systems operate.

- 2.1.2. United States. General Accounting Office. “Critical Infrastructure Protection: Challenge and Efforts to Secure Control Systems.” GAO-04-354. Mar. 2004. Washington, DC. Available Online: <[www.gao.gov/new.items/d04354.pdf](http://www.gao.gov/new.items/d04354.pdf)>.

Review performed by the GAO examining the problems in control systems security, specifically SCADA, and the relationship of these systems to CI management and protection. Examines the vulnerabilities of these systems to attack and what has been done, and not done, to protect them.

- 2.1.3. Shaw, William. *Cybersecurity for SCADA Systems*. Tulsa, OK: PennWell, 2006.

An excellent overview text on SCADA, SCADA technology, and computer-based security issues in SCADA environments. Covers basic concepts and detailed technical risks and approaches.

**2.2**

- 2.2.1. Nash, Troy. “Backdoors and Holes in Network Perimeters.” US-CERT Control Systems Security Center. Case Study Series Vol. 1.1 (2005). Available Online <[www.us-cert.gov/control\\_systems/pdf/backdoor0503.pdf](http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf)>.

- 2.2.2. Nash, Troy. “An Undirected Attack Against Critical Infrastructure.” US-CERT Control Systems Security Center. Case Study Series Vol. 1.2 (2005). Available Online <[www.us-cert.gov/control\\_systems/pdf/undirected\\_attack0905.pdf](http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf)>.

Both of the Nash publications (2.2.1 and 2.2.2) examine the underlying vulnerabilities of network infrastructures to attack. One covers specific attacks against networks and the impacts of these attacks, the other the impact of undirected or general network attacks against CI in a network connected environment.

- 2.2.3. United States. Cong. House. Committee on Governmental Reform. *Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure*. Hearing, 30 Mar. 2004. 108<sup>th</sup> Cong. 2<sup>nd</sup> Sess. Available Online: <[http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.52&filename=95799.pdf&directory=/disk2/wais/data/108\\_house\\_hearings](http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.52&filename=95799.pdf&directory=/disk2/wais/data/108_house_hearings)>.

An industry specific analysis regarding SCADA.

- 2.2.4. Permann, May Robin, and Kenneth Rohde. “Cyber Assessment Methods.” *InTech* 1 Nov. 2005. Available Online:

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

<[http://www.isa.org/InTechTemplate.cfm?Section=Article\\_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=49890](http://www.isa.org/InTechTemplate.cfm?Section=Article_Index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=49890)>.

An overview of SCADA environment testing and certification procedures with a list of practical step and resources for systems administrators and managers.

## 2.3

- 2.3.1. Nuclear Regulatory Commission. *Three Mile Island: A Report to the Commissioners and to the Public*. Washington, DC: 1980. 1-26.

This is the final report from the NRC on Three Mile Island. The recommended sections are the introduction and description of the event, including the non-technical aspects of the failure. The full report is a fascinating reading on SCADA and operational failures.

- 2.3.2. U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the U.S. and Canada*. Apr. 2004. 1-22. Available Online: <<https://reports.energy.gov/BlackoutFinal-Web.pdf>>.

- 2.3.3. Sweet, William. “The Blackout of 2003.” *IEEE Spectrum*. Aug. 2003. Available Online: <<http://www.spectrum.ieee.org/print/3536>>.

Both reading 2.3.2 and 2.3.3 cover the 2003 NE U.S. blackout of the electric power grid. What is interesting is the proximal technical cause, driven by management decision-making, would only have created a localized outage if the system operators had different information and operating assumptions.

- 2.3.4. Foster, John S., et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report*. Washington, DC: Report to Congress, 2004. Available Online: <[http://www.globalsecurity.org/wmd/library/congress/2004\\_r/04-07-22emp.pdf](http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf)>.

An EMP can cause systemic damage to all electronic circuits, including those used in SCADA systems. This is a report of a governmental commission that examined the impact of an EMP on control systems in the public and private sector and the general scope of impact of an EMP attack on the U.S.

- 2.3.5. United States. Cong. *Testimony of Vice Admiral Hyman George Rickover, Naval Nuclear Propulsion Program--1972-73*. Hearing, 8 Feb. 1972 and 28 Mar. 1973. 92<sup>nd</sup> Cong., 1<sup>st</sup> Sess. Washington, DC: Govt. Print. Office, 1974. 1-35.

In contrast to the private sector nuclear programs, the U.S. Navy has had an extraordinary safety and operational record. Admiral Rickover, who is credited with creating and then running the U.S. Navy’s program personally interviewed all officers in the program and oversee the training of the personnel. Rickover’s congressional testimony includes the program details and his philosophy on personnel and operational excellence.

## 2.4

- 2.4.1. Nuclear Regulatory Commission. *Three Mile Island: A Report to the Commissioners and to the Public*. Washington, DC: 1980. 89-108, 161-164.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

This is the final report from the NRC on Three Mile Island. The recommended section is the summary of observations and recommendations, and it covers both the technical and more importantly the non-technical aspects of the failure. There are key discussions on both accounting and management decisions and recommendations on how to improve training. Additionally, the report offers an interesting contrast to the Rickover testimony.

- 2.4.2. Schneier, Bruce. “Non-Security Considerations in Security Decisions.” Workshop on Economics and Information Security, 29-30 May 2003. Available Online: <[ww.cpppe.umd.edu/rhsmith3/papers/Final\\_session6\\_schneier.pdf](http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_schneier.pdf)>.

Schneier, a well-respected cryptologist, discussed the human factors in technical security systems. Having created and broken numerous codes and security systems, he presents in his slides the major vulnerability in the systems, the human element.

**Module 2 Supplementary Readings:**

- \* Farrell, Alexander E., Hisham Zerriffi, and Hadi Dowlatabadi. “Energy Infrastructure and Security.” *Annual Review of Environment and Resources* 29 (Nov. 2004): 421-469. Available Online: <[arjournals.annualreviews.org/doi/pdf/10.1146/annurev.energy.29.062403.102238](http://arjournals.annualreviews.org/doi/pdf/10.1146/annurev.energy.29.062403.102238)>.

A review of energy systems, the control systems that manage them, and their increasing vulnerability in the age of terrorism.

- \* Manto, Charles L. “Introduction to EMP All-Hazards Public Safety Planning and Emerging Requirements for 9-1-1 Emergency Communications Centers.” Public Technology Institute, 2006. Available Online: <[http://www.pti.org/Chicago\\_may06\\_presentations/EMP\\_Scenario\\_for\\_All\\_Hazards.pdf](http://www.pti.org/Chicago_may06_presentations/EMP_Scenario_for_All_Hazards.pdf)>.

A good overview of the impacts of an EMP and the impact on telecommunications systems used in emergencies.

- \* Foster, John S., et al. “Preliminary Findings of the Commission to Assess the Threat from High Altitude Electromagnetic Pulse.” Washington, DC: 2004. Available Online: <[empcreport.ida.org/3militaryVGversionJuly.pdf](http://empcreport.ida.org/3militaryVGversionJuly.pdf)>.

A good presentation to accompany the other EMP document from the Commission with illustrations and documentation of risks from an EMP and the offensive and defensive strategies associated with its use.

- \* United States. Department of Homeland Security. Computer Emergency Readiness Team (US-CERT). *Overview of Cyber Vulnerabilities*. Available Online: <[http://www.uscert.gov/control\\_systems/csvuls.html](http://www.uscert.gov/control_systems/csvuls.html)>.

US-CERT provides a technical introduction to control system vulnerability, focusing on common architecture and potential means of undertaking malicious action.

- \* United States. Department of Homeland Security. Idaho National Laboratory. “Control Systems Cyber Security Defense in Depth Strategies.” May 2006. Available Online: <<http://csrc.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf>>.

The security of control systems previously was assumed to be a product of isolation (separation of control systems from other corporate computing networks) and technical specificity (unique software and

## Critical Infrastructure and Control Systems Security Curriculum

### Appendix B – Annotated Bibliography

hardware with characteristics that were not widely known). However, the pursuit of increased economic efficiency have led control systems to be increasingly interconnected with larger networks that support multiple functions (and are open to a greater number of users) and reliant on standardized components with known vulnerabilities. The report discusses the “end of security by obscurity” and outlines the contours of the contemporary risk environment within which control systems reside. The report focuses attention on mitigation strategies designed to take into consideration the changing nature of the threats to and vulnerabilities of control systems.

- \* United States. Department of Homeland Security. Idaho National Laboratory. “Mitigations for Security Vulnerabilities Found in Control System Networks.” 2006. Available Online: <<http://csrp.inl.gov/Documents/MitigationsForVulnerabilitiesCSNetsISA.pdf>>.

On-site assessments routinely reveal shortcomings in the implementation and operation of security measures associated with control systems. DHS established the Control Systems Security Center at Idaho National Laboratory (INL) to improve on these failings. The report describes observed on-site vulnerabilities and presents mitigation strategies. The report underscores the difficulty of reducing questions of control system security to either a problem of technical design or organizational management.

- \* United States. Department of Homeland Security. Idaho National Engineering and Environmental Laboratory. “A Comparison of Oil and Gas Segment Cyber Security Standards.” Nov. 2004. Available Online: <[http://www.uscert.gov/control\\_systems/pdf/oil\\_gas1104.pdf](http://www.uscert.gov/control_systems/pdf/oil_gas1104.pdf)>.

- \* United States. Department of Homeland Security. Idaho National Engineering and Environmental Laboratory. “A Comparison of Electrical Sector Cyber Security Standards and Guidelines.” Oct. 2004. Available Online: <[http://www.us-cert.gov/control\\_systems/pdf/electrical\\_comp1004.pdf](http://www.us-cert.gov/control_systems/pdf/electrical_comp1004.pdf)>.

These two reports offer examinations of different approaches to security within particular CI sectors. The reports detail varying approaches in an effort to allow the reader to assess the merits of each approach. The readings are particularly useful for students interested in sector-specific questions or operation.

- \* Nelson, Trent. “Common Control System Vulnerability.” United States. Department of Homeland Security. Idaho National Laboratory. Nov. 2005. Available Online: <[http://www.us-cert.gov/control\\_systems/pdf/csvul1105.pdf](http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf)>.

Nelson’s report, prepared under the sponsorship of INL and DHS, discusses common sources of control system vulnerability as well as a number of possible mitigation strategies. The report is focused on intentional disrupts resulting from attacks that allow malicious individuals to compromise safe system functioning.

- \* Brown, Alan S. “SCADA vs. the Hackers.” *Mechanical Engineering*. Dec. 2002. Available Online: <[www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html](http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html)>.

A non-technical introduction to the problems associated with contemporary control systems (they were designed without consideration of intentional disruption, often piggyback on other networks, are left unsecured, conduct real-time processes that cannot be locked down, rely on products that are increasingly standardized with widely known exploits, etc.). The article also provides mention of some notable events and possible attack scenarios.

### Module 3: Managing Organizations and Risk

#### 3.1.

- 3.1.1. La Porte, Todd R. “Challenges of Assuring High Reliability When Facing Suicide Terrorism.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 99-120.

La Porte senior is a principal of the Berkeley research group that began the study of highly reliable organizations in the 1980s. This piece lays out what we know about such organizations, and discusses the extraordinary challenges they face from terrorist operations.

- 3.1.2. Weick, Karl E., Kathleen M. Sutcliffe, Robert E. Quinn. *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. New York: John Wiley & Sons, 2001. 1-84.

A highly readable account of how highly reliable or “mindful” organizations work to reduce failures, with an eye to developing some business principles that may be useful guides to organization managers.

#### 3.2.

- 3.2.1. La Porte, Todd M. “Organizational Strategies for Complex Systems Resilience, Reliability, and Adaptation.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 35-153.

La Porte junior provides an overview of organization theories and strategies that are applicable to CIP operations, and policy suggestions that flow from them.

- 3.2.2. Perrow, Charles. “Complexity, Coupling and Catastrophe” and “Living with High Risk Systems.” *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, 1984/1999. 62-100; 304-352.

A classic in the field, Perrow lays out the kernel of his theory of “normal accidents,” which he argues are the inevitable, though not necessarily common, result of complex organizations that are structured in specific ways.

- 3.2.3. Wildavsky, Aaron. “Anticipation and Resilience” and “The Secret of Safety Lies in Danger.” *Searching for Safety*. New Brunswick, NJ: Transaction Books, 1988. 77-95; 205-228.

Another classic piece, Wildavsky argues that strategies of anticipation of harm can actually be more costly and less protective in the long run than strategies that emphasize resilience. Anticipation works best when threats are known and predictable and where adversaries do not learn. Resilience is indicated when threats are more variable and where adaptation to changing conditions is necessary.

#### 3.3.

- 3.3.1. Schulman, P.R., E. Roe, M. van Eeten, and M. de Bruijne. “High Reliability and the Management of Critical Infrastructures.” *Journal of Contingencies and Crisis Management* 12.11. (2004): 14-28. Available Online: <<http://www.blackwell-synergy.com/toc/jccm/12/1>>.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

Schulman, Roe, and colleagues investigate what helped California power managers keep the lights on during the electricity crisis of 2001. They find that “reliability professionals,” people who improvise to work around system design flaws, were essential, but not widely understood or appreciated.

- 3.3.2. Roe, E., et. al. 2002. *California’s Energy Restructuring: The Challenge to Providing Service and Grid Reliability*. EPRI, Palo Alto, California Energy Commission, Sacramento, CA. rpt. no. 1007388 (Dec. 2002). Available Online: <<http://my.epri.com/portal/server.pt?>>.

An outstanding detailed look at how the California electric power system, which had undergone substantial redesign under deregulation, dealt with the shock of severe weather and unanticipated market activities, evolving quickly from a traditional orderly market to a “real-time network.” This case is an important foundation for the training exercise in this module.

- 3.3.3. U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the U.S. and Canada*. Apr. 2004. 1-173. Available Online: <<https://reports.energy.gov/BlackoutFinal-Web.pdf>>.

An additional crucial report that describes the overall functioning of the North American grid from a technical point of view, and the causes of the world’s largest blackout yet experienced.

### 3.4.

- 3.4.1. Perrow, Charles. “Organizing to Reduce the Vulnerabilities of Complexity.” *Journal of Contingencies and Crisis Management* 7.3 (1999): 150-156. Available Online: <<http://blackwell-synergy.com/toc/jccm/7/3>>.

Perrow provides clear and succinct suggestions to reduce vulnerabilities to large-scale system failures, such as the Northeast blackout and terrorist attacks in 2001. Suggestions include inelegant, perhaps less-efficient, but robust designs that build in redundancy rather than retrofit it later, a high degree of organizational transparency, and strong rewards for error reporting and most important developing extensive external stakeholders to keep risky systems honest.

- 3.4.2. United States. National Aeronautics and Space Administration. *Final Report of the Columbia Accident Investigation Board*. vol. 1. Washington, DC: 2003: chapters 5-8, 11. Available Online: <<http://www.caib.us>>.

One of the best official investigations of a technical disaster ever conducted, this study provides an exceptionally rich discussion of technical, organizational, and cultural *factors* in the destruction of the Columbia space shuttle. It marries theoretical insights to close attention to engineering reality.

- 3.4.3. Rochlin, Gene. 1997. *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton, NJ: Princeton University Press. Full text available at <<http://www.pupress.princeton.edu/books/rochlin/>>. See especially chapters 10-12.

Rochlin provides insightful detail through several case studies of the implications of technical designs that rely heavily on highly automated control systems, systems, which reduce organizational slack to a minimum, but also keep humans increasingly out of the loop. This type of system design, Rochlin argues, has serious consequences for organizations that have to deal with unforeseen contingencies.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

**Module 3 Supplementary Readings:**

- \* La Porte, Todd. R., and Paula Consolini. “Working in Practice But Not in Theory: Theoretical Challenges of ‘High Reliability’ Organizations.” *Journal of Public Administration Research and Theory* 1.1 (1991): 19-48.

The classic theoretical statement of the problem of organizations that operate risky technologies in high-tempo situations and, nevertheless, achieve extraordinary levels of reliable operation. So-called “high reliability organizations” pose important challenges to organization theory and to society: given that society depends increasingly on highly reliable operations. Is it prepared to assume their stringent conditions of functioning, including their high cost? The article describes common features of such organizations and outlines research questions for further study.

- \* Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, 1984/1999.

The clearest articulation of the thesis that tightly-coupled, centralized organizational systems operating complex and hazardous technologies face a non-zero risk of system failure (according to a normal probability distribution). Given that the breakdown of some such systems, such as nuclear power generation, could cause catastrophic damage to society, it is argued that society should consider abandoning them in favor of systems that are inherently less hazardous and more amenable to human organizational control. Book shows through case studies of nuclear power, petrochemicals, marine transport, air traffic, dams and mines, and others on how the way they are organized contributes to catastrophic failures.

- \* Grabowski, Martha and Karlene Roberts. “Risk Mitigation in Large-Scale Systems: Lessons from High Reliability Organizations.” *California Management Review* 39.4 (Summer 1997): 152-162.

Examines the propensity of risk to “migrate” to places in large, complex, and interdependent technical systems that are out of managerial or operational view, with potentially catastrophic consequences for overall system functioning.

- \* Comfort, Louise K. “Institutional Re-orientation and Change: Security as a Learning Strategy.” *The Forum* 1.2 (2002): Article 4. Available Online: <<http://www.bepress.com/forum/vol1/iss2/art4>>.

This article challenges the top-down approach to homeland security adopted by the new federal department. It argues instead that decentralized, “auto-adaptive” approaches emphasizing communication across agencies and jurisdictions are likely to improve overall response to threats and attacks.

- \* Perrow, Charles. “Shrink the Targets.” *IEEE Spectrum* (Sep. 2006). Available Online: <<http://spectrum.ieee.org/sep06/4423>>.

Argues that natural and technological disasters are far more costly than terrorist attacks.

The national priority should be to reduce our vulnerabilities to natural and technological disasters, and in so doing we will reduce our exposure to the threat of terrorism.

- \* Langewiesche, William. “Columbia’s Last Flight.” *The Atlantic Monthly* 292.4 (Nov. 2003): 58-87. Available Online: <<http://www.theatlantic.com/doc/prem/200311/langewiesche>>.

A companion to NASA’s Columbia accident report, Langewiesch’s article discusses the shuttle catastrophe and the investigation.

## Module 4: Securing Networks of Enterprises

### 4.1.

- 4.1.1. Amin, M. “National Infrastructures as Complex Interactive Networks.” *Automation, Control, and Complexity: An Integrated Approach*. Eds. Tariq Samad & John Weyrauch. New York: John Wiley & Sons, 2000. 263-286. Available Online: <[160.94.126.215/amin/Amin\\_Chapter14.pdf](http://160.94.126.215/amin/Amin_Chapter14.pdf)>.

Amin examines large-scale national infrastructures, such as power and telecommunications, as complex networks. This suggests they demonstrate many of the characteristics of complex systems. The non-linearity of these systems complicates their design, operations, and analysis.

- 4.1.2. Kinsey, Jean. “A Faster, Leaner, Supply Chain: New Uses of Information Technology.” *American Journal of Agricultural Economics* 82.5 (Dec. 2000): 1123-1129. Available Online: <<http://www.blackwell-synergy.com/doi/abs/10.1111/0002-9092.00109#search=%22A%20Faster%2C%20Leaner%2C%20Supply%20Chain%3A%20New%20Uses%20of%20Information%20Technology%22>>.

An overview of supply chains across multiple industry actors, taken from a non-technical sector (agriculture), but examining how information technology impacts the performance of a complex supply chain, with a case study of Wal-Mart. This illustrates the vulnerability of long supply chains, especially those heavily reliant on IT.

- 4.1.3. U. S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the U.S. and Canada*. Apr. 2004. Available Online: <<https://reports.energy.gov/BlackoutFinal-Web.pdf>>. 131-153.

This is the final report of the U.S./Canadian Task Force examining the 2003 blackout of the electric power grid. This section covers the principal recommendations, including considering the complexity of the grid and management issues that might complicate the operations and maintenance of the network.

- 4.1.4. Sheffi, Yossi. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press, 2005. 115-136; 270-285.

Supply chains are the classic example of interdependent infrastructures. The two assigned chapters from a book documenting a three-year MIT study, address "Reducing the Likelihood of Intentional Disruptions" and the final chapter seeking to make the case that reducing supply chain vulnerability may not impact a firm's competitiveness, notwithstanding some degree of impact on inventory costs.

### 4.2.

- 4.2.1. Carlson, J.M., and John Doyle. “Complexity and Robustness.” *Proceedings of the National Academy of Sciences of the United States of America* 99.3 Suppl. 1 (2002): 2538-2545. Available Online: <[http://www.pnas.org/cgi/reprint/99/suppl\\_1/2538](http://www.pnas.org/cgi/reprint/99/suppl_1/2538)>.

A basic primer on the concepts of complexity and robustness. An underlying thesis in the course is that systems supporting critical infrastructures require a degree of robustness to create sufficient reliability. The trade-off between optimization and reliability is explored as well as the concepts behind complexity.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

- 4.2.2. United States. Department of Energy. *21 Steps to Improve Cyber Security of SCADA Networks*. Washington, DC: 2002. Available Online: <[www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf](http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf)>.

A quick guide, from the USDOE, on the vulnerabilities of SCADA networks and how best to address them. Interesting in part because of the generic nature of the recommendations and that most are non-technical. This highlights the underlying risks to these networks coming not from technology per se, but how it is implemented and managed.

- 4.2.3. United States. Cong. House. Committee on Governmental Reform. *Telecommunications and SCADA: Secure Links or Open Portals to the Security of the Nation's Critical Infrastructure*. Hearing, 30 Mar. 2004. 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. Available Online: <[http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.52&filename=95799.pdf&directory=/disk2/wais/data/108\\_house\\_hearings](http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.52&filename=95799.pdf&directory=/disk2/wais/data/108_house_hearings)>.

- 4.2.4. St. Sauver, Joe. “SCADA Security and Critical Infrastructure.” Eugene, OR: Infragaurd Meeting, 7 Dec. 2004. Available Online: <<http://www.uoregon.edu/~joe/>>.

This PowerPoint presentation provides an overview of SCADA, some history of its vulnerabilities and how these have been exploited by the U.S. during the cold war, and how they might be exploited by those that wish to damage CI in the U.S. Case study of facilities in the NW U.S. along with some simple and compelling perspectives on SCADA history and futures.

### 4.3

- 4.3.1. Nishiguchi, Toshihiro, and Alexandre Beaudet. “Self-Organization and Clustered Control in the Toyota Group: Lessons from the Akin Fire.” International Motor Vehicle Program, Massachusetts Institute of Technology, 1997. Available Online: <[imvp.mit.edu/papers/98/167a.pdf](http://imvp.mit.edu/papers/98/167a.pdf)>.

The Toyota automotive group developed a robust supply system built on organizational relationships as much as technology. This paper examines the impacts of this management approach in responding to a single-point failure in the Akin fire and how the system recovered.

- 4.3.2. Lawler, Andrew. “Faster, Cheaper, Better on Trial.” *Science* 288.5463 (2000): 32-34. Available Online: <<http://www.sciencemag.org/cgi/content/full/288/5463/32>>.

This brief piece from Science Magazine looks at technology management at NASA and the failures and successes of a new management approach. An important story about organizational process change and the often large distance between theory and practice in management and its impacts.

- 4.3.3. Chatfield, Carl, and Timothy Johnson. *Microsoft Office Project 2003: Step by Step*. Redmond, WA: Microsoft Press, 2004.

SW manual to help users prepare for the exercise. Focus on simple data entry and creation of PERT like charts to illustrate the concept of critical path.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

#### 4.4

- 4.4.1. Greenstein, Shane M. “The Economic Geography of Internet Infrastructure in the United States.” Working Paper #0046. Center for the Study of Industrial Organization, Northwestern University. Available Online: <[http://siepr.stanford.edu/programs/SST\\_Seminars/CSIO-WP-0046.pdf](http://siepr.stanford.edu/programs/SST_Seminars/CSIO-WP-0046.pdf)>.

A good overview of the technical and organizational topology of the Internet in the U.S. As more and more systems are connected to the public Internet, even through firewalls and other security tools, we increase the risk of control system compromise. The goal of this reading is to sensitize the student to the risks of the public network and why security experts recommend avoiding public network connection where feasible.

- 4.4.2. Peterson, Dale, Matt Franz, and Landon Lewis. *SCADA Security*. Available Online: <[http://www.digitalbond.com/SCADA\\_Blog/SCADA\\_blog.htm](http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm)>.

Overview of SCADA security issues in complex networks.

- 4.4.3. Gordon, Lawrence A., Martin A. Loeb, and William Lucyshyn. “Economic Aspects of Controlling Capital Investments in Cyberspace Security for Critical Infrastructure Assets.” 2<sup>nd</sup> Annual Workshop on Economics and Information Security, University of Maryland (2003). Available Online: <[www.cpppe.umd.edu/rhsmith3/papers/Final\\_session7\\_lucyshyn.loeb.gordon.pdf](http://www.cpppe.umd.edu/rhsmith3/papers/Final_session7_lucyshyn.loeb.gordon.pdf)>.

This paper evaluates the tradeoffs of making investments in technical security and the risks of compromise of critical control systems. The basic challenge of management is making this risk/investment decision regarding critical infrastructures while operating in a competitive business environment. Using a model-based approach, they demonstrate that security investments have a positive NPV.

- 4.4.4. Garcia, Alfredo, and Barry Horowitz. “The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy.” The Fifth Workshop on the Economics of Information Security, Cambridge, UK (2006). Available Online: <[weis2006.econinfosec.org/docs/24.pdf](http://weis2006.econinfosec.org/docs/24.pdf)>.

Communications networks increase with complexity as they grow in scale and scope. As the Internet has grown and its importance to commerce and public safety increased, the security investments needed to improve reliability and security have also increased. There exists potential for operators to under invest in security for their Internet networks with a high probability of compromise or failure.

#### **Module 4 Supplementary Readings:**

- \* Emerson, Cole H. “The Kobe Earthquake: Assessing Your Risk.” *Disaster Resource Guide* 1996. Available Online: <[http://www.disaster-resource.com/articles/kobe\\_eq\\_emerson.shtml](http://www.disaster-resource.com/articles/kobe_eq_emerson.shtml)>.

A brief article examining the Kobe earthquake and the damage it caused in supply chains, amongst other damage, and the resiliency of some of the systems. This document covers the Toyota/Sumitomo relationship on brake shoe supply.

- \* Sheffi, Yossi. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press, 2005.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

This book reports the results of a three-year study at MIT of supply chain vulnerabilities and speaks to how a variety of companies have increased resilience or reduced vulnerability in ways that can, arguably, be cost justified. The highly readable book is crammed with interesting anecdotes, based on extensive fieldwork by the MIT team. From this point of view alone, a quick read of the book will be rewarding. It addresses the role of government tangentially.

## Module 5: Creating Markets

### 5.1.

- 5.1.1. Hahn, Robert W., and Paul C. Tetlock. "Introduction to Information Markets." *Information Markets: A New Way of Making Decisions*. Eds. Robert W. Hahn and Paul C. Tetlock. Washington, DC: AEI-Brookings Joint Center for Regulatory Studies, 2006. 1-12. Available Online: <<http://www.aei-brookings.org/admin/authorpdfs/page.php?id=1304>>.

This chapter provides a readable introduction to information markets, describing issues of design, accuracy of predictions, and implementation.

- 5.1.2. Berg, Joyce E., and Thomas A. Rietz. "The Iowa Electronic Markets: Stylized Facts and Open Issues." *Information Markets: A New Way of Making Decisions*. Eds. Robert W. Hahn and Paul C. Tetlock. Washington, DC: AEI-Brookings Joint Center for Regulatory Studies, 2006. 142-169. Available Online: <<http://www.aei-brookings.org/admin/authorpdfs/page.php?id=1310>>.

This paper reviews experience with the Iowa Electronic Markets, small-scale, real money futures markets conducted by the University of Iowa College of Business. The best known of these is the Iowa Political Markets, in which contracts are designed so that prices can be used to predict election outcomes. Such markets have been found to generate predictions whose accuracy compares favorably with alternative approaches.

- 5.1.3. Hanson, Robin. "Designing Real Terrorism Futures." *Public Choice* (forthcoming).

The paper addresses theoretical and practical considerations in the design of speculative markets in order to make specific predictions about terrorist attacks. Design issues considered include combinatorics (dealing with a very large number of possible scenarios), manipulation, moral hazard, hiding prices, decision selection bias (the bias what occurs when traders expect decision makers to know more than traders do).

- 5.1.3. Shachtman, Noah. "The Case for Terrorism Futures" *Wired* 30 Jul. 2003. Available Online: <<http://www.wired.com/news/politics/0,1283,59818,00.html>>.

This article describes politics and issues behind the debate over the Policy Analysis Market funded by the Defense Advanced Research Projects Agency (DARPA).

### 5.2.

- 5.2.1. Chichilinsky, Graciela. and Geoffrey. M. Heal. "Managing Unknown Risks: the Future of Global Reinsurance." Working Paper # PW-97-07. Columbia Business School, Aug. 1997. Available Online: <<http://www.columbia.edu/cu/business/wp/>>.

The paper discusses the use of financial markets and insurance to manage catastrophic risks, such as resulting from climate change or terrorism. The authors discuss approaches combining the risk pooling capacity of insurance with the diversification and hedging potential of securities markets.

- 5.2.2. Heal, Geoffrey M, and Howard Kunreuther. "You Only Die Once: Managing Discrete Interdependent Risks." Cambridge, MA: National Bureau of Economic Research, 2003. Available Online: <<http://www.nber.org/papers/w9885>>.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

This paper considers the general problem of inter-dependent security (one person's security depends on the actions of others) in the context of low-frequency, high-impact events. The authors present a theoretical model and then propose a set of risk management solutions including insurance, liability, taxation, regulation and third-party inspections, and coordinating mechanisms.

- 5.2.3. Dixon, Lloyd, and Robert Reville. "National Security and Private-Sector Risk Management for Terrorism." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 292-304.

Historically, government programs and policies have attempted to share the costs of and provide compensation for a host of different forms of risk. Dixon and Reville focus on the role that the government can play in addressing a newly identified source of risk: terrorism. The chapter argues that terrorism, the work of purposeful actors, differs significantly from many other forms of risk and, consequently, calls for public and private partnerships. Terrorism insurance and compensation are becoming issues of national security, this chapter outlines why this is the case and defines the possible actions that can be taken as a result.

- 5.2.4. Macdonald, James W. "Terrorism, Insurance, and Preparedness: Connecting the Dots." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 305-337.

Before September 11, 2001, domestic terrorism was considered by insurers to be an unlikely occurrence that could be covered without any additional premium. The staggering losses sustained on September 11, 2001, dashed this notion and called into question the ability of insurance markets to adequately address the risk posed by the threat of terrorism. Macdonald focuses on the interrelated issues of preparedness, perception of risk, and pricing in arguing for a long-term federal role in shaping and supporting terrorism insurance.

### 5.3.

- 5.3.1. Experimental economics exercises hosted by the University of Virginia. Available Online: <<http://veconlab.econ.virginia.edu/admin.htm>>.

In particular:

Prediction markets: <<http://veconlab.econ.virginia.edu/psm/psm.php>>.

Reciprocity games: <<http://veconlab.econ.virginia.edu/rg/rg.php>>.

Public good game: <<http://veconlab.econ.virginia.edu/pg/pg.php>>.

- 5.3.2. Kormos, Michael, and Thomas Bowe. "Coordinated and Uncoordinated Crisis Responses by the Electric Power Industry." *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 194-210.

Kormos and Bowe draw from the events of September 11, 2001, and the August 14, 2003, blackout to illustrate the challenges that confront operators in achieving greater resilience and efficiency of the national electric infrastructure. As interdependencies both within and across infrastructure services increase, coordinated response becomes indispensable. In this chapter, the authors discuss some of the institutions and practices that are currently working toward this end.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

- 5.3.3. Feinstein, Jack. “Managing Reliability in Electric Power Industries.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerwald et al. New York: Cambridge UP, 2006. 164-193.

Feinstein provides an introduction into the workings of electric power companies and focuses on sources of vulnerability and ways to ensure reliability. The chapter argues that management failures are at the root of most blackouts and that an inability to learn from the mistakes of the past can pose a significant hazard to continued reliability.

- 5.3.4. Roe, E., et. al. *California’s Energy Restructuring: The Challenge to Providing Service and Grid Reliability*. EPRI, Palo Alto, California Energy Commission, Sacramento, CA. rpt. no. 1007388 (Dec. 2002). ix-xix; ch. 7-9. Available Online: <<http://my.epri.com/portal/server.pt?>>.

Prior to the California energy crisis, the system’s slogan was “Reliability through Markets.” The essence of the crisis was the failure of market mechanisms. The authors detail the collapse of the market, and the institutional and organizational responses to that collapse that allowed service provision to continue. In light of the experience of power providers during the crisis, the authors further describe how the standards defining reliable service provision are in the process of revision. The authors detail sixteen factors driving electric power operations from planned to “real-time” operations, and argue for the institutionalization of such fallback mechanisms to ensure future high reliability in California’s energy sector.

#### 5.4.

- 5.4.1. Epstein, Paul, and Evan Mills (eds.). “Financial Implications, Scenarios, and Solutions.” *Climate Change Futures: Health, Ecological, and Economic Dimensions*. Report of the Center for Health and the Global Environment, Harvard Medical School, 2005. 92-111. Available Online: <[http://chge.med.harvard.edu/research/ccf/documents/ccf\\_final\\_report.pdf](http://chge.med.harvard.edu/research/ccf/documents/ccf_final_report.pdf)>.

Global climate change creates new environmental and public health threats. This report details the nature of these threats in three categories: infectious and respiratory disease, extreme weather events, and natural and managed systems. The assigned part of the report addresses both the manner in which climate change is creating new challenges for financial institutions, and the manner in which financial instruments may be used to mitigate the emergent threats that are ensuing.

- 5.4.2. Baranoff, Dalit. “A Policy of Cooperation: the Cartelisation of American Fire Insurance, 1873–1906.” *Financial History Review* 10 (2003): 119–136. Available Online: <<http://journals.cambridge.org/action/displayFulltext?type=1&fid=190204&jid=&volumeId=&issueId=02&aid=190203>>.

When producers or service providers organize, substituting cooperation for competition, a static model of markets predicts that the public will be adversely affected through restricted output and higher prices. This paper describes in detail a historical case in which cartelization of the fire insurance market—while indeed resulting in higher prices to consumers—also enabled robust risk sharing and an improved overall resilience of the industry. The author describes the manner in which the increased resilience of the industry was manifest in the rapid recovery that followed the Baltimore fire of 1904 and the San Francisco earthquake and fire of 1906.

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

**Module 5 Supplementary Readings:**

- \* Lakdawall and Zanjani. “Insurance, Self-protection, and the Economics of Terrorism.” RAND Working Paper #WR-171-icj. Jul. 2004. Available Online: <[http://www.rand.org/pubs/working\\_papers/2005/RAND\\_WR171.pdf](http://www.rand.org/pubs/working_papers/2005/RAND_WR171.pdf)>.

This working paper deals with the question surrounding public intervention into the terrorism insurance market. The authors note that public intervention has been unusually aggressive both domestically and internationally when compared to other areas. They offer both normative and positive discussion, determining that public intervention is warranted due to the presence of negative externalities associated with interdependent security and private protection. They also offer a seemingly quixotic observation: “In some cases private investment in security or protection has negative externalities (for example, not investing in rebuilding lower NYC has negative effects with respect to morale?)” and suggest that public intervention in terrorism markets here mimics war insurance (providing incentives to engage in risky behaviors).

- \* Woo, G. “Quantifying Insurance Terrorism Risk.” Prepared for the National Bureau of Economic Research, Cambridge MA, 1 Feb. 2002. Online: <[www.rms.com/NewsPress/Quantifying\\_Insurance\\_Terrorism\\_Risk.pdf](http://www.rms.com/NewsPress/Quantifying_Insurance_Terrorism_Risk.pdf)>.

Woo considers the possibility of creating probabilistic models upon which insurance policy can be based (in other words, how can the risk of terrorism be quantified?). Woo concludes that it is possible to build formal models based in part on expert judgment and subjective inputs (that is on modeling ex ante, without ex post results to buttress calculation).

- \* Stevens, Gina Marie. “Homeland Security Act of 2002: Critical Infrastructure Information Act.” CRS Report RL31762. 2003. Available Online: <[ftp.fas.org/sgp/crs/RL31762.pdf](http://ftp.fas.org/sgp/crs/RL31762.pdf)>.

The report discusses the tension between voluntary industry information disclosure to federal authorities and open government. Specifically, the discussed proposed legislation seeks to exempt particular forms of information submitted and processed by DHS to the FOIA. The report details the different sections of legislation.

- \* Gorman, Sean P. “A Cyber Threat to National Security?” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et. al. New York: Cambridge UP, 2006. 239-257.

The importance of cyber security to national security is richly contested: some argue that it is a key site of vulnerability waiting to be exploited, while others argue that the threat is largely illusory. Gorman enters into this debate by exploring possible credible threats and the effect of CI failure. Gorman considers physical failures (both intentional and unintentional), malicious cyber attacks, and cyber warfare capabilities. The survey puts into context the question of cyber security, illustrating how the pursuit of efficiency forges new sources of vulnerability and the threat of cyber terrorism remains both real and difficult to quantify. The chapter concludes with a discussion of the role that public policy could play in closing the gap between the safety the public demands and security the private sector provides.

- \* Knight, Frank H. “Enterprise and Profit.” *Risk, Uncertainty, and Profit*. New York: Kelly and Millman, 1933/1957. 264-313.

Knight’s classic discusses the role of uncertainty and risk in economic life. The chapters suggested here argue that uncertainty, the inability to know without reservation the outcome of a given situation, gives

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

rise to profit and organizational structure. Knight's discussion is relevant today, touching on the relationship between uncertainty and enterprise, responsibility and control, and imperfect knowledge in a dynamic world. Much of the discussions of the relationship between the workings of the market and assessments of risk owe a debt to Knight's path-breaking work.

- \* Viscusi, W. Kip, and Richard J. Zeckhauser. "The Perception and Valuation of the Risks of Climate Change: A Rational and Behavioral Blend." Working Paper #RWP05-062. Kennedy School of Government, Harvard University, Nov. 2005. Available Online: <[http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP05-062/\\$File/rwp\\_05\\_062\\_zeckhauser\\_SSRN.pdf](http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP05-062/$File/rwp_05_062_zeckhauser_SSRN.pdf)>.

Previous public surveys have assessed in general terms the extent of public concern regarding adverse impacts of climate change. This paper reports results of a more detailed survey quantitatively assessing risk perceptions related to climate change. Respondents were graduate students in law and public policy. The survey tests a set of behavioral hypotheses concerning the ability to assess risks from high-uncertainty, high-impact events.

- \* Berkley, Seth. "Ending an Epidemic: The International AIDS Vaccine Initiative Pioneers a Public-Private Partnership." *Innovations* 1.1 (2006): 52-66. Available Online: <<http://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2006.1.1.52>>.

A private firm developing a new vaccine faces considerable scientific and regulatory uncertainties. Even if a vaccine is successfully developed, particular characteristics of the vaccine market may limit returns. Furthermore, while conferring private benefits, vaccines for infectious diseases are also public goods: when one person uses a vaccine, they also lower the risk of disease transmission to others in the population. The case study describes the development of the International AIDS Vaccine Initiative (IAVI) a path-breaking effort to address these paired market failures. By coordinating research efforts and mobilizing pre-commitments for purchases, IAVI seeks to accelerate the development of a vaccine for HIV-AIDS, the only pathway for eradication of the disease.

- \* Glennerster, Rachel, Michael Kremer, and Heidi Williams. "Creating Markets for Vaccines," *Innovations* 1.1 (2006): 67-79. Available Online: <<http://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2006.1.1.67>>.

In the context of a discussion of the case of the International AIDS Vaccine Initiative (see Berkley 2006, listed above), the authors describe the particular market failures that reduce private incentives to develop vaccines. The authors detail a particular proposal to spur the creation of new vaccines through credible advance purchase commitments by governments other large public entities.

## Module 6. Building Trust – Public/Private Policy

### 6.1.

- 6.1.1. Auerswald, Philip E., Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. “Leadership: Who Will Act? Integrating Public and Private Interests to Make a Safer World.” *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Eds. Philip Auerswald et al. New York: Cambridge UP, 2006. 483 –505.

The concluding chapter of this book summarizes the “take-away” messages and a series of recommendations and discussion of what may be required to ensure that the reliability of critical services keeps pace with their growing complexity and interdependence. It focuses primarily on public policy issues, both domestic and international, recognizing that both government and the private sector are international in their reach and dependencies.

- 6.1.2. Bush, George W. *National Strategy for Combating Terrorism*. Washington, DC: 5 Sep. 2006. Available Online: <<http://www.whitehouse.gov/nsc/nsct/2006/>>.

These two views (6.1.2 and 6.1.3) of where the U.S. government stands and is headed are in sharp contrast, one, the president’s most recent view and the next, a skeptical view from the journalist John Gershman.

- 6.1.3. Gershman, John. “A Secure America in a Secure World.” FPIF Task Force on Terrorism. *Foreign Policy In Focus* (Sep. 2004). Available Online: <<http://www.fpif.org/papers/04terror/index.html>>.

- 6.1.4. Lovins, Amory B., L. Hunter Lovins, and Alec Jenkins. “Achieving Resilience.” *Brittle Power: Energy Strategy for National Security*. Andover MA: Brick House Publishing Cop., 1982. 293 – 334.

This last chapter (co-authored with Alec Jenkins) of the book introduced in the first module addresses the public policy issues seen from the perspective of 1982. It urges a long-term shift in infrastructure technologies, based on the author’s quest for resilience and their passion for each citizen playing a role in bringing about the needed changes.

### 6.2.

- 6.2.1. Michel-Kerjan, Erwann, and Nathalie de Marcellis-Warin. “Public-Private Programs for Covering Extreme Events: The Impact of Information Distribution on Risk Sharing.” *Asia-Pacific Journal of Risk and Insurance* 1.1 (2006): 21-49. Available Online: <[opim.wharton.upenn.edu/risk/downloads/06-08-EMK.pdf](http://opim.wharton.upenn.edu/risk/downloads/06-08-EMK.pdf)>.

Information sharing among firm, industries, cross-industry links and government (local, state, national and transnational) is critical to building trust, which in turn is critical to the collaboration on which safety and security depends in times of disaster.

### 6.3.

- 6.3.1. Abele-Wigert, Isabelle, and Myriam Dunn. *International CIIP Handbook 2006: An Inventory of Protection Policies in 20 Countries and 6 International Organizations*. Vol. 1. Zurich: Center for Security Studies, ETH, 2006. Available Online:

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

<<http://se2.isn.ch/serviceengine/FileContent?serviceID=PublishingHouse&fileid=5A4EB000-B539-72C4-A2A8-1107EADBA271&lng=en>>.

This reading, a comprehensive documentation of how 20 nations are dealing with critical information infrastructure vulnerability and protection provides the background for the class exercise, which looks at the relative approaches of nations and institutions and evaluates their merits.

**6.4.**

- 6.4.1. Carter, Ashton. “The Architecture of Government in the Face of Terrorism.” *International Security* 26.3 (Winter 2001/02): 5–23. Available Online: <[http://muse.jhu.edu/journals/international\\_security/v026/26.3carter.html](http://muse.jhu.edu/journals/international_security/v026/26.3carter.html)>.

Is the U.S. government structure prepared to deal with the broad spectrum of terrorist threats including those against CI? This practical evaluation by a national security expert is companion piece to Donahue on new modes of collaborative government, read in the first module.

- 6.4.2. Farmer, Richard D. “Homeland Security and the Private Sector.” Washington, DC: Congressional Budget Office, Dec. 2004. Available Online: <[www.cbo.gov/ftpdoc.cfm?index=6042&type=1](http://www.cbo.gov/ftpdoc.cfm?index=6042&type=1)>.

This excellent analysis from the CBO gives a legal and policy perspective on the relationship between public and private sectors in the quest for homeland security.

- 6.4.3. Committee on Science and Technology in Countering Terrorism, National Research Council. “Essential Partners in a National Strategy: States and Cities, Industry, and Universities.” *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academies Press, 2002. 357-371. Available Online: <<http://newton.nap.edu/catalog/10415.html>>.

The recognition, shortly after September 11, 2001, that trust and cross-sector and public-private cooperation are essential, and points to some of the obstacles to achieving that cooperation.

**Module 6 Supplementary Readings:**

- \* Kunreuther, Howard, Heal, Geoffery, and Orszag, Peter R. “Interdependent Security for Homeland Security Policy and Other Areas.” Brookings Institution Policy Brief #108. Online: <<http://www.brook.edu/comm/policybriefs/pb108.htm>>.

The brief provides a short introduction of the problems of interdependent security using airline security as a general example. The brief considers the role of public intervention and sketches a number of different possible remedies (collaborative action, taxation, insurance, liability). In conclusion, the authors suggest a mixed plan that uses public policy to create private incentives for action through insurance and third party inspection.

- \* Howitt, Arnold M, and Robyn L. Pangi, Eds. *Countering Terrorism: Dimensions of Preparedness*. Cambridge, MA: MIT Press, 2003.

An edited collection covering four broad areas: strategies and institutions; emerging threats; capacity building; and lessons learned from international cases. The essays cover a wide-breadth, focusing on institutional arrangements that foster ill-prepared capacity to combat terrorism, the specific threats posed

Critical Infrastructure and Control Systems Security Curriculum  
Appendix B – Annotated Bibliography

by bio, cyber, nuclear, and agricultural terrorism, other international cases (Japan, UK, Israel), and the unique challenges that the health care, communication, and legal communities face from terrorism.

\* Dunn, Myriam, and Victor Mauer, eds. *International CIIP Handbook 2006: Analyzing Issues, Challenges, and Prospects*. Vol. 2. Zurich: Center for Security Studies, ETH, 2006. Available Online: <[http://www.crn.ethz.ch/publications/crn\\_team/detail.cfm?id=16157](http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157)>.

Vol. 2 of the CIIP Handbook discusses the unique challenges that confront CI and CII (Critical Information Infrastructure). The book draws from an international perspective (see reading assignment for Module 6, Session 3) and considers the changing economics of infrastructure service, the role of public institutions in protection, and the need for collaboration both across sectors and regions.

**Appendix C**  
**Key Government Reports**

## Appendix C

### Key Government Reports

Bush, George W. *National Strategy for Combating Terrorism*. Washington, DC: 5 September 2006. Available Online: <<http://www.whitehouse.gov/nsc/nsct/2006/>>.

United States. Commission on National Security/21<sup>st</sup> Century (the Hart-Rudman Commission). 3 Vols. Major Themes and Implications. Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom. Road Map for National Security: Imperative for Change. 1998-2001. Available Online: <<http://www.au.af.mil/au/awc/awcgate/nssg/>>.

United States. Committee on Science and Technology in Countering Terrorism, National Research Council. *Making the Nation Safer: the Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academies Press, 2002. Available Online: <<http://newton.nap.edu/catalog/10415.html>>.

United States. Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC: 2006. Available Online: <[http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIPP\\_Plan.pdf](http://www.dhs.gov/dhspublic/interweb/assetlibrary/NIPP_Plan.pdf)>.

United States. Department of Homeland Security. *National Response Plan*. Washington, DC: 2004. Available Online: <[http://www.dhs.gov/dhspublic/interweb/assetlibrary/NRP\\_FullText.pdf](http://www.dhs.gov/dhspublic/interweb/assetlibrary/NRP_FullText.pdf)>.

United States. National Aeronautics and Space Administration. *Final Report of the Columbia Accident Investigation Board*. vol. 1. Washington, DC: 2003. Available Online: <<http://www.caib.us>>.

U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the U.S. and Canada*. Apr. 2004. Available Online: <<https://reports.energy.gov/BlackoutFinal-Web.pdf>>.

United States. National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. Washington, DC: Government Printing Office, 22 Jul. 2004. Available Online: <<http://www.9-11commission.gov/report/index.htm>>.

United States. National Science and Technology Council, Interagency Working Group on Cyber Security and Information Assurance. *Federal Plan for Cyber Security and Information Assurance Research and Development*. Washington, DC: Apr. 2006. Available Online: <[http://www.nitrd.gov/pubs/csia/csia\\_federal\\_plan.pdf](http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf)>.

United States. Presidential Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructure*. (The Marsh Report) Washington, DC: 1997. Available Online: <[www.fas.org/sgp/library/pccip.pdf](http://www.fas.org/sgp/library/pccip.pdf)>.

United States. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. *Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. Washington DC: Government Printing Office, 15 Feb. 2006. Available Online: <[http://katrina.house.gov/full\\_katrina\\_report.htm](http://katrina.house.gov/full_katrina_report.htm)>.